Security Protocols for Mobile Ubiquitous E-Health Systems

Autor: *Pablo Picazo Sánchez*

Directores: *Dr. Pedro Peris López*
Dr. Juan M. Estévez Tapiador

Firma del Tribunal Calificador:

Presidente:

Vocal:

Secretario:

Calificación:

Leganés, de de

A mis padres

Abstract

Wearable and implantable medical devices constitute an already established industry nowadays. According to a recent research [113], North America is currently the most important market followed by Europe, Asia-Pacific and the rest of the world. Additionally, the same document remarks the importance of the Asia-Pacific region due to the rising ageing population and the overpopulation in that area. The most common implantable medical devices include pacemakers, defibrillators, cochlear implants, insulin pumps, and neurostimulators among others.

In recent years, the proliferation of smartphones and other mobile "smart" devices with substantial computational and communication capabilities have reshaped the way wireless body area network may be implemented. In their current generation (or in a near future), all of them share a common feature: wireless communication capabilities [127]. Moreover, implantable medical devices have the ability to support and store telemetry data facilitating the remote monitoring of the patient. Medical devices can be part of a wireless body area network, operating both as sensors and as actuators and making decisions in real time.

On the other hand, a new kind of devices called wearables such as smart bracelets or smart watches have been equipped with several sensors like Photoplethysmogram (PPG) to record the heart beats, accelerometers to count the steps or Global Positioning System (GPS) to geopositioning users and were originally conceived as cheap solutions to help people to improve their workout. However these devices have demonstrated to be quite useful in many healthcare environments due to a huge variety of different and low-cost medical sensors. Thus, patients can be monitored for long periods of time without interfering in their daily life and taking their vital signs constantly under control.

Security and privacy issues have been described as two of the most challenging problems of implantable medical devices and, more generally, wireless body area networks [6, 47, 84, 103]. As an example, it has been demonstrated that somebody equipped with a low cost device can eavesdrop on the data exchanged between a reader and a peacemaker and may even induce a cardiac arrest [71]. Health-related data have been the focus of several attacks almost since the adoption of computers in the healthcare domain. As a recent example, in 2010 personal data from more than 26 millions of veterans were stolen from the Department of Veterans Affairs' database in the US by an employee who had access to the database [104]. The Ponemon Institute pointed out that Germany and the US spent in 2013 more than $7.56 and $11 millions, respectively, to protect personal health records from attacks.

This PhD dissertation explores the security and privacy of data in healthcare environments where confidential information is measured in real time by some sensors placed in, on, or around the human body. Security and privacy in medical conditions have been widely studied by the research community, nonetheless with the recent boom of wearable devices, new security issues have arisen.

The first part of this dissertation is dedicated to the introduction and to expose both the main motivation and objectives of this PhD Thesis. Additionally the contributions and the organization of this document are also presented.

In the second part a recent proposal has been analysed from the security and

privacy points of view. From this study, vulnerabilities concerning to full disclosure, impersonation, traceability, de-synchronization, and Denial-of-Service (DoS) attacks have been found. These attacks make the protocol infeasible to be introduced with an adequate security and sufficient privacy protection level. Finally, a new protocol named Fingerprint$^+$ protocol for Internet of Thing (IoT) is presented, which is based on ISO/IEC 9798-2 and ISO/IEC 18000-6C and whose security is formally verified using BAN logic.

In the third part of this dissertation, a new system based on International Standard Organization (ISO) standards and security National Institute of Standards and Technology (NIST) recommendations have been proposed. First, we present a mutual entity authentication protocol inspired on ISO/IEC 9798 Part 2. This system could be deployed in a hospital where Radio Frequency IDentification (RFID) technology may be used to prune blood-handling errors, i.e., the identities of the patients and blood bags are confirmed (authentication protocol) and after that the matching between both entities is checked (verification step). Second, a secure messaging protocol inspired on ISO/IEC 11770 Part 2 and similar to that used in electronic passports is presented. Nowadays the new generation of medical implants possess wireless connectivity. Imagine a doctor equipped with a reader aims to access the records of vital signals stored on the memory of an implant. In this scenario, the doctor (reader) and the patient (implant) are first mutually authenticated and then a secure exchange of data can be performed.

The fourth part of this Thesis provides an architecture based on two cryptographic protocols, the first one is for publishing personal data in a body area network composed of different sensors whereas the second one is designed for sending commands to those sensors by guaranteeing the confidentiality and fine-grained access control to the private data. Both protocols are based on a recently proposed public cryptography paradigm named ciphertext policy attribute-based encryption scheme which is lightweight enough to be embedded into wearable devices and sensors. Contrarily to other proposals made on this field, this architecture allows sensors not only to encrypt data but also to decrypt messages generated by other devices.

The fifth part presents a new decentralized attribute based encryption scheme named Decentralized Ciphertext-Policy Attribute Based Searchable Encryption that incorporates ciphertext-policy attribute-based encryption with keyword search over encrypted data. This scheme allows users to (a) encrypt their personal data collected by a Wireless Body Area Network (WBAN) according to a policy of attributes; (b) define a set of keywords to enable other users (e.g., hospital stuff) to perform encrypted search over their personal (encrypted) data; (c) securely store the encrypted data on a semi-honest server and let the semi-honest server run the (encrypted) keyword search. Note that any user can perform a keyword query on the encrypted data, however the decryption of the resulting ciphertexts is possible only for users whose attribute satisfy the policy with which the data had been encrypted. We state and prove the security of our scheme against an honest-but-curious server and a passive adversary. Finally, we implement our system on heterogeneous devices and demonstrate its efficiency and scalability

Finally, this document ends with a conclusions achieved during this PhD and a summary of the main published contributions.

Keywords: Security, Privacy, Cryptography, eHealth.

Resumen

Los dispositivos médicos implantables como los marcapasos o las bombas de insulina fueron concebidas originalmente para controlar automáticamente ciertos parámetros biológicos y, llegado el caso, poder actuar ante comportamientos anómalos como ataques cardíacos o episodios de hipoglucemia. Recientemente, han surgido uno dispositivos llamados *wearables* como las pulseras cuantificadoras, los relojes inteligentes o las bandas pectorales. Estos dispositivos han sido equipados con un número de sensores con capacidad de monitorizar señales vitales como el ritmo cardíaco, los movimientos (acelerómetros) o sistemas de posicionamiento (GPS) entre otros muchas opciones, siendo además una solución asequible y accesible para todo el mundo.

A pesar de que el propósito original fue la mejora del rendimiento en actividades deportivas, estos dispositivos han resultado ser de gran utilidad en entornos médicos debido a su amplia variedad de sensores. Esta tecnología puede ayudar al personal médico a realizar seguimientos personalizados, constantes y en tiempo real del comportamiento de los pacientes, sin necesidad de interferir en sus vidas cotidianas.

Esta Tesis doctoral está centrada en la seguridad y privacidad en entornos médicos, donde la información es recogida en tiempo real a través de una serie de sensores que pueden estar implantados o equipados en el propio paciente. La seguridad y la privacidad en entornos médicos ha sido el foco de muchos investigadores, no obstante con el reciente auge de los *wearables* se han generado nuevos retos debido a que son dispositivos con fuertes restricciones de cómputo, de memoria, de tamaño o de autonomía.

En la primera parte de este documento, se introduce el problema de la seguridad y la privacidad en el paradigma de Internet de las cosas y haciendo especial hincapié en los entornos médicos. La motivación así como los principales objetivos y contribuciones también forman parte de este primer capítulo introductorio.

La segunda parte de esta Tesis presenta un nuevo protocolo de autenticación basado en RFID para IoT. Este capítulo analiza previamente, desde el punto de vista de la seguridad y la privacidad un protocolo publicado recientemente y, tras demostrar que carece de las medidas de seguridad suficientes, un nuevo protocolo llamado Fingerprint$^+$ compatible con los estándares de seguridad definidos en el estándar ISO/IEC 9798-2 y EPC-C1G2 (equivalente al estándard ISO/IEC 18000-6C) ha sido propuesto.

Un nuevo sistema basado en estándares ISO y en recomendaciones realizadas por el NIST ha sido propuesto en la tercera parte de esta Tesis. En este capítulo se presentan dos protocolos bien diferenciados, el primero de ellos consiste en un protocolo de autenticación basado en el estándar ISO/IEC 9798 Part 2. A modo de ejemplo, este protocolo puede evitar problemas de compatibilidad sanguínea, es decir, primero se confirma que el paciente es quien dice ser y que la bolsa de sangre realmente contiene sangre (proceso de autenticación). Posteriormente se comprueba que esa bolsa de sangre va a ser compatible con el paciente (proceso de verificación).

El segundo de los protocolos propuestos consiste en un protocolo seguro para el intercambio de información basado en el estándar ISO/IEC 11770 Part 2 (el mismo que los pasaportes electrónicos). Siguiendo con el ejemplo médico, imaginemos que un doctor equipado con un lector de radiofrecuencia desea acceder a los datos que un dispositivo implantado en el paciente está recopilando. En este escenario tanto el lector como el implante, se deben autenticar mutuamente para poder realizar el intercambio de información de manera segura.

En el cuarto capítulo, una nueva arquitectura basada en el modelo de *Publish/-Subscribe* ha sido propuesto. Esta solución está compuesta de dos protocolos, uno para el intercambio de información en una red de área personal y otro para poder reconfigurar el comportamiento de los sensores. Ambos protocolos están diseñados para garantizar tanto la seguridad como la privacidad de todos los datos que se envían en la red. Para ello, el sistema está basado en un sistema de criptografía de clave pública llamado *Attribute Based Encryption* que es suficientemente ligero y versátil como para ser implementado en dispositivos con altas restricciones de cómputo y de memoria.

A continuación, en el quinto capítulo se propone una solución completamente orientada a entornos médicos donde la información que los sensores obtienen de los pacientes es cifrada y almacenada en servidores públicos. Una vez en estos servidores, cualquier usuario con privilegios suficientes puede realizar búsquedas sobre datos sifrados, obtener la información y descifrarla. De manera adicional, antes de que los datos cifrados se manden a la nube, el paciente puede definir una serie de palabras claves que se enlazarán a los datos para permitir posteriormente búsquedas y así obtener la información relacionada a un tema en concreto de manera fácil y eficiente.

El último capítulo de esta Tesis se muestran las principales conclusiones obtenidas así como un resumen de las contribuciones científicas publicadas durante el período doctoral.

Palabras Clave: Seguridad, Privacidad, Criptografía, eHealth.

Contents

List of Figures

List of Tables

Acronyms

6LoWPAN	IPv6 over Low power Wireless Personal Area Network.
ABE	Attribute Based Encryption.
ABSE	Attribute Based Searchable Encryption.
AES	Advanced Encryption Standard.
aMSE-DDH	augmented Multi-Sequence of Exponents Decisional Diffie-Hellman.
API	Application Programming Interface.
BAN	Body Area Network.
BLE	Bluetooth Low Energy.
CCA	Chosen-Ciphertext Attack.
CMAC	Cipher-based MAC.
CPA	Chosen-Plaintext Attack.
CP-ABE	Ciphertext Policy Attribute Based Encryption.
CPU	Central Processing Unit.
CRC	Cyclic Redundancy Code.
DCP-ABE	Decentralized Ciphertext Policy Attribute Based Encryption.
DoS	Denial-of-Service.
ECG	Electrocardiogram.
EEG	Electroencephalography.
EHR	Electronic Health Record.
EPC	Electronic Product Code.
EPC-C1G2	EPC Class-1 Generation-2.
FID	Fixed Input Data.
GPRS	General Packet Radio Service.
GPS	Global Positioning System.
GSM	Global System for Mobile communication.
GSR	Galvanic Skin Response.
HABE	Hierarchical Attribute-Based Encryption.

HIBE	Hierarchical Identity-Based Encryption.
HL7	Health Level 7 consortium.
IBE	Identity Based Cryptography.
ICT	Information and Communication Technology.
IMD	Implantable Medical Device.
IoT	Internet of Thing.
IPv6	Internet Protocol version 6.
ISO	International Standard Organization.
KDF	Key Derivation Function.
KGC	Key Generation Center.
KP-ABE	Key-Policy Attribute Based Encryption.
LBAC	Lattice-Based Access Control.
LSSS	Linear Secret Sharing Scheme.
MA-ABE	Multi-Authority Attribute Based Encryption.
MAC	Message Authentication Code.
NFC	Near Field Communication technology.
NIST	National Institute of Standards and Technology.
PEKS	Public Encryption with Keyword Search.
PGP	Pretty Good Privacy.
PHR	Personal Health Record.
PP-ABE	Privacy Preserving Attribute-Based Encryption.
PPG	Photoplethysmogram.
PPT	Probabilistic Polynomial Time.
PRF	Pseudorandom Function.
PRNG	Pseudorandom Number Generator.
RBAC	Role-Based Access Control.
RFID	Radio Frequency IDentification.
SCKA	Selective Chosen Keyword Attack.
SE	Searchable Encryption.
SMPC	Secure Multi-Party Computation.
SSE	Searchable Symmetric Encryption.
TA	Trusted Authority.
TTP	Trusted Third Party.
UHF	Ultra High Frequency.
UWB	Ultra-WideBand.

VABKS	Verifiable Attribute-based Keyword Search.
WAN	Wide Area Network.
WBAN	Wireless Body Area Network.
WSN	Wireless Sensor Network.

1

Introduction

1.1 Context

The term IoT refers to a combination of Internet and small objects or devices, usually equipped with a wireless connection, whose main purpose is to sense and react automatically to some previously defined environmental changes [115, 156, 161]. Those devices are known as things and might have some embedded sensors and actuators. In this Thesis, only those devices related to human body surveillance are referenced such as Implantable Medical Devices (IMDs) or wearables, however there are many others such as small device placed somewhere inside the car in charge of taking the driver's eyes under control to stop the car in case she is falling sleep or even a humidity sensor placed under the field to know if the automatic irrigation should be turned on or not.

The IoT was originally inspired by RFID technology which is widely used for tracking applications [97]. However, cooperation and interaction between sensors, actuators, mobiles phones or RFID tags have been demonstrated to be a perfect solution not only for tracking purposes but also for monitoring, automatic data collection and data sharing activities. Smart hospitals, smart cities or smart buildings are only a few examples in which IoT technology is thought to be included.

The proliferation of affordable wearable devices has increased the amount of personal data that can be easily collected, processed and stored. Providing adequate protection to such data has become a challenging task. As an example, in the Six Nations rugby championship 2015, an IoT solution was deployed in a stadium equipped with a WiFi connection and millions of data were measured directly from the players only by wearing some wireless sensors in the shirt, boot, wrist or in a chest band. Moreover, not only anyone equipped with a smartphone with a WiFi connection is able to consume those data in real time from her favourite player but coaches can also track their players to improve their performance [139].

From a more technical point of view, things in IoT are characterized by the next capabilities: connectivity, identification, localization, mobility, hardware constraints, software developments and security and privacy issues. The mentioned capabilities are explained bellow.

Connectivity. Objects have the ability to be connected to Internet or even with other things in the same network. Wireless technologies such as WiFi, RFID, Bluetooth, Near Field Communication technology (NFC), Global System for Mobile communication (GSM), WBAN, ZigBee, General Packet Radio Service (GPRS), Wide Area Network (WAN) or 3G play a key role in the IoT deploy-

ment. Due to the huge amount of new devices that IoT will bring, Internet Protocol version 6 (IPv6) is becoming more and more important in this new paradigm.

Identification. Objects should be unique and identifiable when necessary. This identification process is done physically trough RFID/NFC technologies or by a combination of some attributes which make each device unique.

Localization & Mobility. Another interesting property that things have is the location capability, i.e., objects are always geo-positioned trough GPS, GSM, RFID or WiFi technologies. Furthermore, in a real scenario, objects may move around, joining and leaving new networks and thus handling this mobility is a must in IoT.

Hardware. Current tendency in IoT is to build objects as small as possible without losing any of the capabilities that they already have. For example, when a new wearable is being developed, users' wishes are data security, data storage, different communication protocols, long-life battery, price or the external appearance among many other properties. All these requirements are not easy to be achieved and the research community has a real challenge with IoT.

Software. Objects have a set of chips which can be reconfigured to perform some actions. Many others are equipped with a Central Processing Unit (CPU) and thus developers can develop new algorithms to compute some operations in the own device before doing something else with the information. In other words, objects are thought to collect information about their surroundings, store it, forward it or do some extra actions by developing some artificial intelligence, routing, or security algorithms.

Security & Privacy. Security and privacy issues are described in the literature as one of the most challenging problems that IoT has. Sensors, actuators and personal information must be secured, however there are some physical constraints that must be taken into account like computational, power and memory restrictions that IoT have. Moreover, this is even more dramatic in eHealth[1] environments because devices are measuring personal data which can be stored in external servers and thus, the information should be encrypted once the data is measured in the own device.

According to an European report life expectancy has increased enormously in the last century. In 1900, people were expected to live around 50 years whereas at the end of the century, life expectancy was around 75 and 81 years old for men and women respectively. This increment was originated mainly by the improvements taken in both the communicable diseases at young ages and in cardiovascular diseases [22]. Spain has increased its life expectancy from 72.5 in 1980 to 82.5 in 2012 which gives it the 12th position in the rank of the World Health Organization [163]. Furthermore, if we consider life expectancy over the world, the average has grown from 46.6 years in the 1950s to 67.6 years in 2005.

IMDs are widely used nowadays. Each year more than 300,000 people in the U.S. have at least one of these devices inside their human body and it is estimated that more than 2.5 million people have one of them. One of the most known devices is a

[1]Term used to refer tools and services using Information and Communication Technologys (ICTs)

RFID tag developed by VeriChip Corp. and approved in 2004 to be implantable in the human body. However it is not the only IMD, cardiac pacemakers, defibrillators, neuro stimulators, cochlear implants, drug delivery systems (insulin pumps) or bionic implants are only a subset of these devices. Usually, an external device may set up some IMD parameters and extract stored data via wireless communication.

On the other hand, a new set of devices called wearables have proliferated nowadays as an affordable solution to monitor some biological signals. The most common include smart bracelets, smart watches or smartphones. In their current generation (or in the near future), all of them will share a common feature: wireless communication capabilities [127]. Moreover, both IMDs and wearables have the ability to support and store telemetry data an thus the remote monitoring of the patient will be performed easily.

As an example, devices with telemetry functionalities and more precisely ingestible IMDs equipped with radio frequency antennas have been proposed in several works as a promising option for the gastrointestinal endoscopies [5, 42, 99].

Further to the above considerations, different reports point out that the IMDs and the healthcare IoT market segment are ready to manage about $70 billion in 2018 [155] and $117 billion by 2020, respectively. Applications like fall detection, medical fridges tracking, sportsmen care, patients surveillance or drug administration are only a few examples of the vast possibilities that IoT might contribute to healthcare [114].

In a near future, population age will be increased significantly and, in terms of the economy, the cost of having particular nurses or particular medical doctors to attend patients at home is unaffordable. Population is becoming older and therefore, some mechanism to remote monitoring of vital signals will be a must for those people who need to be constantly monitored but are not kept in the medical center.

Technology, and more particularly IoT, is already playing a main role in healthcare systems and many countries over the world are moving towards eHealth systems to jump the gap between patients' daily life and medical entities such as doctors or care givers. Additionally, eHealth will be quite important in many other situations such as countries in which socio-economical problems do not allow them to improve in their health system or people who have mobility restrictions because of physical or geographical conditions [162]. Despite the union of technology and health systems has generated several challenges [34], eHealth has much more advantages that we would have never imagined such as real-time access to the patients' biosignals and the ability to make decisions for some emergency situations [27], a huge amount of data to research and to improve new drugs or solutions to some diseases.

Apart from the above advantages, eHealth systems are also capable of storing biological signals and forwarding them to a centralized server which might be physically located in a hospital or even in a public cloud server. Important companies such as Microsoft with its project named Microsoft HealthVault or Intel and Dell which are collaborating with Meditech[2] for a healthcare cloud system. Health records store in the cloud are known as Electronic Health Records (EHRs)[3]. This is particularly useful because the researchers, caregivers, medical staff or any other authorized en-

[2]https://ehr.meditech.com/

[3]Also known as Personal Health Records (PHRs)

tity can access to those records at any time and anywhere with the guarantee that those records are always updated and reliable. Additionally, EHRs should also have the possibility to be linked with their owners in case it was necessary.

Server grant access and access by roles should be implemented in order to preserve data privacy, *e.g.*, a cardiologist should be able to access to heart data however she should not access to audiometry data. Nonetheless some more complex scenarios should be taken into account, for example those in which a cardiologist would need some audiometry data. In that case she would ask for permission to an otolaryngologist to be allowed to retrieve that information otherwise she would not have access to that personal information.

There are two different organizations in charge of defining the future standards for eHealth such as security and privacy issues, interoperability of the devices, medical data sharing or the nomenclature of medical data records: the ISO and the Health Level 7 consortium (HL7).

1.2 Motivation and Objectives

In recent years, the proliferation of smartphones and other mobile smart devices with substantial computational and communication capabilities have reshaped the way WBANs may be implemented. WBANs may be defined as a set of networked sensors (they have communication capabilities and can interact with each other and with a central network controller that provides coordination, long-term storage, etc.) which are over a patient and are constantly measuring various health-related parameters. In a more general way, WBANs may be seen as a consequence of the union of IoT and Wireless Sensor Networks (WSNs) technologies applied to the eHealth world [105].

The IoT are extremely vulnerable to attacks because most of the communications are wireless, which makes eavesdropping extremely simple. Also, most of the IoT devices such as RFID tags are characterized by their tight constraints in terms of memory, energy and computing resources. Therefore these devices cannot support on-board complex security algorithms. Apart from the insecurity of using the radio channel the major security problems concern to authentication and data integrity. For example, the theft of newborn children is a worldwide problem that has recently made the news. It is claimed that in the last 50 years more than 300,000 newborns were abducted in Spain [112]. Similar cases have been reported in Australia [51], while in the US the National Center for Missing & Exploited Children has published some statistics about this alarming problem [120]. To address this problem, several hospitals in different countries have adopted a new and controversial RFID-based solution due to the potential benefits that this technology could offer, both in terms of savings in operational costs and as enablers of novel applications [13, 108, 152, 165, 172].

From the security point of view of the personal data, in 2010 more than 26 millions of PHRs of veterans were stolen from the Department of Veterans Affairs' database in the US by an employee who had access to the server [104]. On the other hand, it has been demonstrated that somebody equipped with a low cost device can eavesdrop on the data exchanged between a pacemaker and a reader may induce

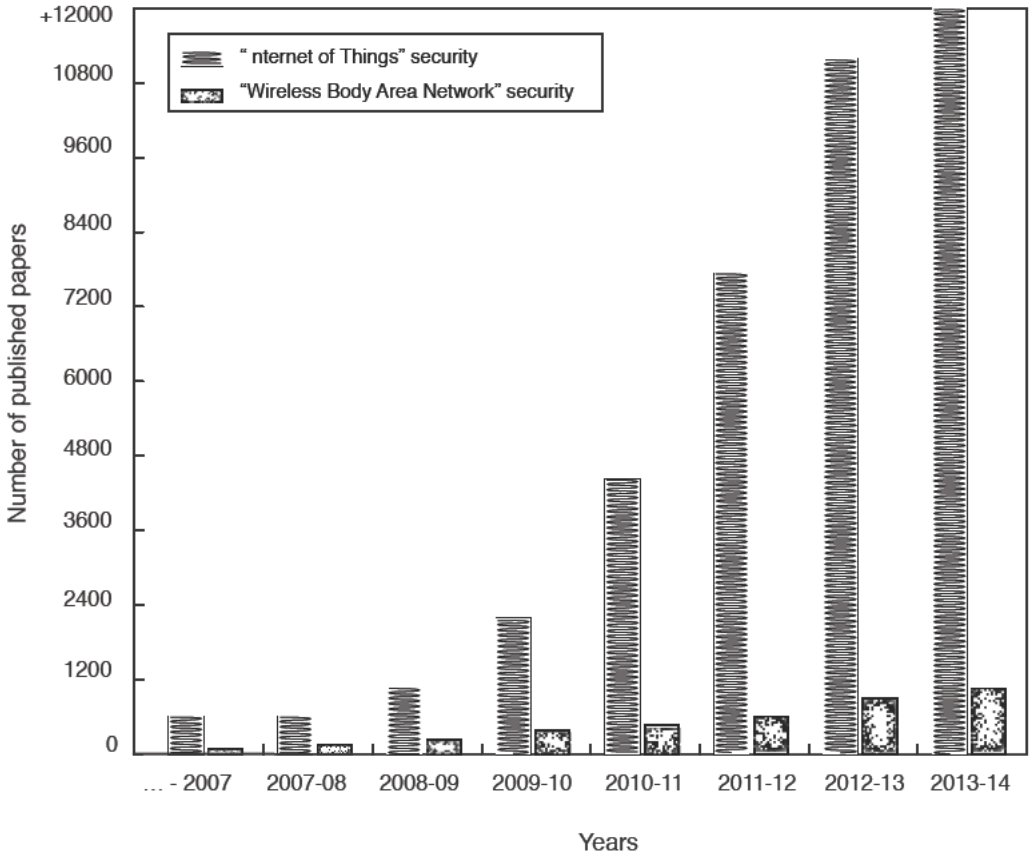


Figure 1.1: Evolution of the number of papers published in Google Scholar[78]

a cardiac arrest [71]. Health-related data have been the focus of several attacks almost since the adoption of computers in the healthcare domain. The Ponemon Institute pointed out that Germany and the US spent in 2013 more than $7.56 and $11 millions, respectively, to protect PHRs from attacks.

Security and privacy issues have been described as two of the most challenging problems of IMDs and, more generally, WBANs [6, 47, 84, 103]. As can be seen in Figure 1.1 researchers have increased their efforts in studying privacy and security aspects of IoT and WBANs. This Thesis dissertation examines security and privacy issues for IoT devices in eHealth environments and more specifically in WBANs.

Firstly, a recent RFID authentication protocol has been analysed and an improvement based on ISO is proposed. Secondly, two recent RFID authentication protocols were cryptanalysed and two new schemes are proposed for IoT and eHealth environments respectively. Thirdly, a new security schema based on Attribute Based Encryption (ABE) for WBANs is developed. Fourthly, a complete system for WBANs where personal data can be retrieved from a database by looking for a given keyword is designed. In particular, this Thesis is focused on the following main objectives:

O1. Analyse an RFID authentication protocol recently published for IoT and proposed an improvement based on an ISO standard.

O2. Design RFID authentication protocols based on different ISO standards and

security recommendations for IoT systems and more specifically for healthcare environments.

O3. Create a suitable model to exchange data securely on a WBAN where all sensors may encrypt and decrypt data. Additionally a mechanism to send command operations to the sensors should be developed in order to allow device reconfiguration in a secure way.

O4. Develop a complete system for eHealth system where PHRs are encrypted and stored on an external server where users may retrieve a subset of PHRs by performing encrypted queries to the database.

1.3 Main Contributions

During this PhD several contributions in the field of security and privacy on WBANs have been published. As a result of the achievement of the aforementioned objectives four main contributions have been accomplished:

C1. The IoT is an emerging paradigm which is used to link physical objects with Internet. One of the most common ways of communicating and identifying objects on IoT is using RFID systems between different objects. Researchers have focused on developing improvements of RFID authentication protocols that stave off privacy threats and well-known security problems. Recently, Khor *et al.* [93] have proposed a new authentication protocol which conforms to the EPC Class-1 Generation-2 (EPC-C1G2) standard (equivalently ISO/IEC 18000-6C). In Chapter 2 the vulnerabilities of this authentication protocol concerning to full disclosure, impersonation, traceability, de-synchronization, and DoS attacks are shown. These attacks make the protocol infeasible to introduce it with an adequate security and sufficient privacy protection level. Finally, we present a new protocol, called Fingerprint$^+$ protocol, which is based on ISO/IEC 9798-2 and ISO/IEC 18000-6C and whose security is formally verified using BAN logic. This work was published in the *Security and Communication Networks* journal [135] .

C2. RFID systems are widely used in access control, transportation, real-time inventory and asset management, automated payment systems, etc. Nevertheless, the use of this technology is almost unexplored in healthcare environments, where potential applications include patient monitoring, asset traceability and drug administration systems, to mention just a few. RFID technology can offer more intelligent systems and applications, but privacy and security issues have to be addressed before its adoption. This is even more dramatic in healthcare applications where very sensitive information is at stake and patient safety is paramount. Wu *et al.* [164] have recently proposed a new RFID authentication protocol for healthcare environments. In Chapter 3 is shown that this protocol puts location privacy of tag holders at risk, which is a matter of gravest concern and ruins the security of this proposal. To facilitate the implementation of secure RFID-based solutions in the medical sector, two new applications (authentication and secure messaging) are suggested and we propose solutions that in contrast to previous proposals in this field, are fully

based on ISO Standards and NIST Security Recommendations. This research culminated in an article published in the *Journal of Medical Systems* [134].

C3. A complete secure architecture to share private data for IMDs and wearables on a WBANs is proposed. The WBAN is thus viewed as a shared bus where a number of entities produce data and subscribe to the data feed provided by other entities. In Chapter 4, two protocols for publishing data and sending commands to a sensor that guarantee confidentiality and fine-grained access control are presented. These protocols are based on a kind of public cryptography called ABE and more specifically CP-ABE scheme which is lightweight enough to be embedded into wearable sensors as it has been demonstrated in [69]. In a more general way, the versatility offered by CP-ABE primitives is used to allow sensors to subscribe to the data feeds published by other sensors. The privileges required to access each particular data are set by the sensor's policy, who can vary them depending on the context. This allows for a flexible, scalable, and highly versatile architecture where services can be dynamically composed by subscribing to the data feeds published by wearable sensors. Apps and external users (*e.g.*, healthcare staff) can get access to such data feeds and also reconfigure or request specific data from the sensors provided that they have sufficient privileges to do so. Finally, the experimental results confirm that the scheme is suitable for most current sensors, including ARM-based platforms. This research led to a publication in the *Sensors* journal [137].

C4. An original decentralized attributed based encryption scheme named Decentralized Ciphertext-Policy Attribute Based Searchable Encryption is presented In Chapter 5. This scheme combines encrypted keyword search and ciphertext policy attribute based encryption. This scheme is suitable for e-Health scenarios, as it allows patients to associate multiple keywords to the encrypted data collected by a WBAN. The encrypted data could then be stored in a cloud server together with the encrypted keyword. Subsequently, the healthcare staff could query the server to run a keyword search and retrieve the desired data. Decryption, however, would still depend on the attributes that the staff possesses. Keyword secrecy and Ciphertext secrecy assure the confidentiality of both the query and the stored data. Finally, the experiments show that all algorithms used in our system can be implemented on highly constrained devices such as smartphones or ARM-based architectures. This research is submitted to an international conference (Asia CCS'16) and it is still under review.

1.4 Organization

The remainder of the document is composed by 4 chapters distributed as follows:

Chapter 2 presents a new RFID authentication protocol named Fingerprint$^+$ for IoT. This chapter analyses an authentication protocol proposed in the literature, and after demonstrating that it is not secure enough an improved version and ISO/IEC 9798-2 and EPC-C1G2 standards compliant is presented.

Chapter 3 introduces two original RFID protocols, an authentication and a secure

messaging protocols for eHealth environments. This chapter surveys the current ISO standards for RFID, analyses the security and privacy of an authentication protocol proposed recently and an improved version following some NIST recommendations and the ISO/IEC 9798 and 11770 ISO standards is proposed.

Chapter 4 explores the use of ABE in WBAN architecture for healthcare scenarios. In this chapter a complete architecture is proposed where sensors can either publish new measured data or subscribe to other sensors' publications. Contrarily to other recent proposals in this field, in our scheme sensors are able to encrypt and decrypt messages according to an access policy. Additionally an authentication protocol is presented to send commands to the sensors and thus reconfigure their behaviour.

Chapter 5 proposes a complete solution based on a decentralized attribute based encryption with keyword search in the context of e-Health systems where two different access policies must be satisfied, one to perform the query and another one to decrypt the data stored in a public database.

Chapter 6 summarizes the main conclusions arisen from this PhD Thesis. Finally, a list of the published papers related to this dissertation is also presented.

2

Weaknesses of Fingerprint-based Mutual Authentication Protocol

2.1 Introduction

The IoT is an emerging paradigm that links Internet with objects (things). The term things is referred to sensors, actuators, RFID tags or smart phones among others devices which communicate through the radio channel. In the last years advances and consolidation of IoT have been the focus of many research work. Most of these projects point out the need to improve security and privacy for the widespread use of this technology ([9, 91, 156, 161]). Additionally, new mechanisms for secure networking have been proposed at [124], [143] and [60]. Readers are urged to consult [9] in which a survey of IoT is presented. In particular in this chapter we deal with a novel fingerprint-based RFID authentication protocol presented by Khor *et al.* in [93].

RFID is a technology that enables identification from distance ([159]) and is already used for a large number of different applications, from cards used for building access or payments with mobile devices ([130]) to applications in sanitary environments ([23]). RFID is widely used over the world and actually is seen from another point of view due to its inclusion in the IoT. In Ultra High Frequency (UHF) band, most of the main manufacturers of IoT proposed an identification based on an Electronic Product Code (EPC) ([124]), thus each one of the physical objects hold an RFID tag ([110, 161]).

There are three main components in RFID technology: tags (also known as transponders), readers (also known as interrogators) and databases. Tags are small devices with severe limitations of memory, computation and storage resources, which implies a challenge for supporting security capabilities. Readers are devices with no computation and memory constraints (in comparison with tags) and communicate with tags and the database. Finally a database is used to store private information such as keys and authenticate tags in the system extra information linked with each tag can be stored too.

The Auto-ID Center was set up in 1999 to develop the EPC and related technologies that could be used to identify and track products through the global supply chain. The standard that may be considered as the universal standard for passive UHF RFID tags is EPC-C1G2 ([53]) (ISO/IEC 18000-6C equivalently).

The IoT is extremely vulnerable to attacks because most of the communications are wireless, which makes eavesdropping extremely simple. Also, as previously men-

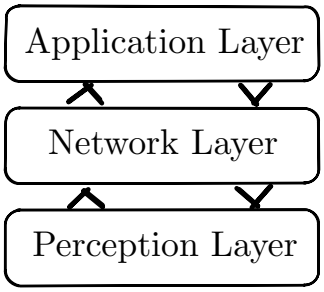


Figure 2.1: IOT Architecture

tioned, most of the IoT entities are characterized by its tight constraints in terms of memory, energy and computing resources. Therefore these devices cannot support on-board complex security algorithms. Apart from the insecurity of using the radio channel the major security problems concern to authentication and data integrity.

2.1.1 Contribution and Organization

Recently, in [93] has been proposed a new mutual authentication protocol which complies with the EPC-C1G2 standard. This chapter brings down the security claimed by the authors in the original paper. In fact the protocol is vulnerable to many well-known security vulnerabilities such as full disclosure, impersonation, traceability, de-synchronization and DoS attacks. It makes Khor *et al.*'s proposal infeasible to be introduced with an adequate security and sufficient privacy protection level.

This chapter is organized as follows. Background and security threats on IoT are introduced in Subsection 2.2. In subsection 2.3 we present the Fingerprint-based Mutual Authentication Protocol. Subsection 2.4 introduces the security weaknesses that the protocol has and wrecks Khor *et al.*'s claims while in subsection 2.5 an improved scheme is presented. This new protocol is based on well-established security standards and its security is formally verified using BAN logic. Finally the chapter ends with some conclusions in subsection 2.6.

2.2 Background and Security Threats

The architecture of an IoT solution is well-established and divided into three different layers (perception, application and network) as can be seen in Figure 2.1.

The perception layer is mainly composed of sensors and actuators, in other words in this layer is where things live. Its function is to identify objects, gather information and interact with the environment.

The application layer is where all logical and software applications live. Databases, social networks, authentication servers, service management or billing functionalities are part of this layer. In other words, this layer constitutes a set of intelligent software application which are applied to the IoT technology to create smart objects.

The network layer is in charge of the information transmission obtained from the perception layer to the application layer. Nowadays the most common way of communication protocols used in IoT are Bluetooth Low Energy (BLE) (in its last version which has been optimized for high constraints devices), Ultra-WideBand (UWB), RFID, NFC, IPv6 over Low power Wireless Personal Area Network (6LoWPAN) and Zigbee standards. Despite having widely used in the research community and in real applications, these standards were not designed from the security and privacy point of view and thus several efforts have been done to secure both data and communications links from the adversaries.

All these technologies are the most common communication systems used to share information between smart things, and external devices. Nevertheless all of them have some characteristics which make them more suitable for some situations than others in terms of range of communications, transmission speed (bps) or the bandwidth they operate. To know more about these wireless technologies two reviews have been published in [15, 179].

The main form of barcode-type RFID device is given by the known EPC standard where four different types of tags are defined: 1) EPC-C1G2 [52], which is the most popular standard for passive RFID tags; 2) Class-2 is a light improvement of EPC-C1G2 where additional memory and authenticated access control are included; 3) Class-3 are known as semi-passive tags and they have a power source to help them with powering the RFID tag when responding to the reader and to provide power to the internal memory; 4) Class-4 are the active tags. They can establish connections by themselves and provide power to the internal memory [136].

Readers are devices with no computation and memory constraints (in comparison with tags) and are the proxy between tags and the databases where the private information is stored and used for recognizing tags (authentication protocols).

As a negative point, RFID tags always respond to reader interrogation while bearers do not have any alert about that communication. Taking that promiscuity into account and the few resources that passive tags have destined to security and privacy issues, guaranteeing the data confidentiality and privacy is one of the main open problems that this technology has [11, 86].

In the last years several classification proposals about security threats in RFID and IoT have appeared in the literature ([11, 92, 98, 115, 117]). We pay particular attention to those done in [117] and [11]. In the first one, authors proposed a classification based on four different RFID layers: strategic, application, network-transport and physical. The attacks were classified basing on the layer where the attack could be conducted, and then the authors proposed possible solutions to combat these ones. Some years later, [11] proposed four main attacks categories that are based on the attack purpose. More precisely he distinguished between impersonation, DoS, information leakage and traceability. Impersonation is a kind of attack in which an adversary is authenticated as another entity without being authorized. For instance, this can be done by replaying messages or tampering the device for acquiring secret information. In a DoS attack the adversary prevents the normal operation of the protocol. This can be achieved by physical manipulation of the channel (jamming) or rendering entities to an unsynchronized state to mention a few examples. Privacy is the main concern of RFID system, which involves data

and localization. Information leakage occurs when private information (data) is disclosed by an adversary. Traceability (localization) is possible when the adversary can link a tag with its responses the tag holder can be tracked. Therefore the tag answer must be changed with each session to avoid traceability attacks moreover correlation between answers has to be negligible.

As shown in [131], the security level of EPC standard is very low or even non-existent. Aiming to increase the security level offered by this standard many proposals ([39, 45, 173, 166]) have been published in the last years, but unfortunately cryptanalysis were published ([72, 90, 132, 177]) in the ensuing months. In this chapter we show how [93] suffers the same fate as previous proposals. That is, this work does not guaranteed the claimed security properties.

2.3 Fingerprint-based Mutual Authentication Protocol

In this section, we show briefly how the authentication protocol proposed by [93] works (see the original paper for details). This protocol was designed conforming to EPC-C1G2 ([53]) and the authors assume that the channel between reader and a back-end server is secure meanwhile between reader and tag is insecure. In fact, this work is marked in the literature ([14, 43, 106, 183]) as a protocol to be followed because of its security and the way it conforms the EPC standard. The definitions of notation used by authors are shown in Table 2.1. The protocol, sketched in Figure 2.2, consists of two main phases: initialization and authentication phase.

2.3.1 Initialization phase

In this first phase, a back-end server stores five values of each tag ($\text{EPC}_{\mathcal{T}}$, FP, DATA, $PRNG$ and K_i) indexed by $[\text{CRC}(\text{EPC}_{\mathcal{T}} \| \text{FP})] \oplus \text{K}_i$. On the other hand, each tag stores three values (K_i, $\text{EPC}_{\mathcal{T}}$ and FP) all of them required to perform authentication.

2.3.2 Authentication phase

In authentication phase, the reader sends a *Request* message to the tag. Then, that tag computes $M_1 = \text{CRC}(\text{EPC}_{\mathcal{T}} \| FP)$ and encrypts M_1 performing a XOR operation between $CRC(\text{EPC}_{\mathcal{T}} \| FP)$ and the session key K_i: $C_k\ (M_1) = [CRC\ (\text{EPC}_{\mathcal{T}} \parallel FP)] \oplus \text{K}_i$. After that, the encrypted message is sent back to the reader and forwarded to the back-end server.

In the server, the authentication of the message is verified. If the decrypted message M_1 does not match with any of the records that the database has, an error message is sent back to the reader. Otherwise, if the message matches a database's record, then the authentication of the tag is successful. At this point, the back-end server generates a temporary key K_s and the tag generates a new temporary key K_t. Finally, the server computes a new message M_2 and sends it back to the tag: $M_2 = CRC(\text{EPC}_{\mathcal{T}} \| FP) \oplus K_s$.

Notation	Interpretation
$\text{EPC}_{\mathcal{T}}$	Tag's EPC
FP	Fingerprint
DATA	Tag Information
CRC()	16-bits Cyclic Redundancy Code (CRC)
$PRNG$	16-bits Pseudorandom Number Generator (PRNG)
K_i	Current session key
K_{i+1}	New session key
K_t	Tag's temporary key
K_s	Server's temporary key
$\oplus$	Bit-wise exclusive OR operation.
$\|\|$	Concatenation
C_k	Cipher
D_k	Decipher
$P \triangleleft MSG1$	P receives $MSG1$
$P\| \sim MSG1$	P sends $MSG1$
$\#(X)$	X is fresh
$P\| \equiv \#(MSG1)$	P believes the freshness of $MSG1$
$\{X\}_K$	Message X is encrypted with the key of K
$P\| \equiv P \overset{K}{\longleftrightarrow} Q$	P believes the secret K is shared between P and Q
$P1 : \frac{P\|\equiv P\overset{K}{\longleftrightarrow}Q, P\triangleleft\{X\}_K}{P\|\equiv Q\|\sim X}$	The message meaning rule of BAN logic that means if P believes that it shares a secret key K with Q and if P receives a message X encrypted with K, then P is entitled to believe that Q once said X. In this chapter we called this rule $P1$
$P2 : \frac{P\|\equiv Q\sim\{X,Y\}}{P\|\equiv Q\|\sim\{X\}}$	This is one rule of BAN logic that means if P believes Q has sent $\{X, Y\}$ then P is entitled to believe that Q has sent X. In this chapter we called this rule $P2$

Table 2.1: Notation used in the Fingerprint-Based Mutual Authentication Protocol

This phase concludes when the tag receives M_2 message from the reader. The tag computes M_t message ($M_t = CRC(\text{EPC}_{\mathcal{T}} \| FP) \oplus K_t$) for verifying the authentication of the back-end server. If M_2 and M_t are equal, the tag updates its session key K_i by $K_{i+1} = PNRG(K_t)$. Otherwise the key is not updated, maintaining the current session key $K_{i+1} = \text{K}_i$ and the tag sends an error message to the back-end server which keeps the old session key too.

2.4 Weaknesses of Khor *et al.* Protocol

In this section, we introduce the security and privacy pitfalls of Khor *et al.*'s protocol. Our analysis ruins the security claims done by the authors. In Table 2.2, the reader can see which the claimed security properties are and those which are not satisfied.

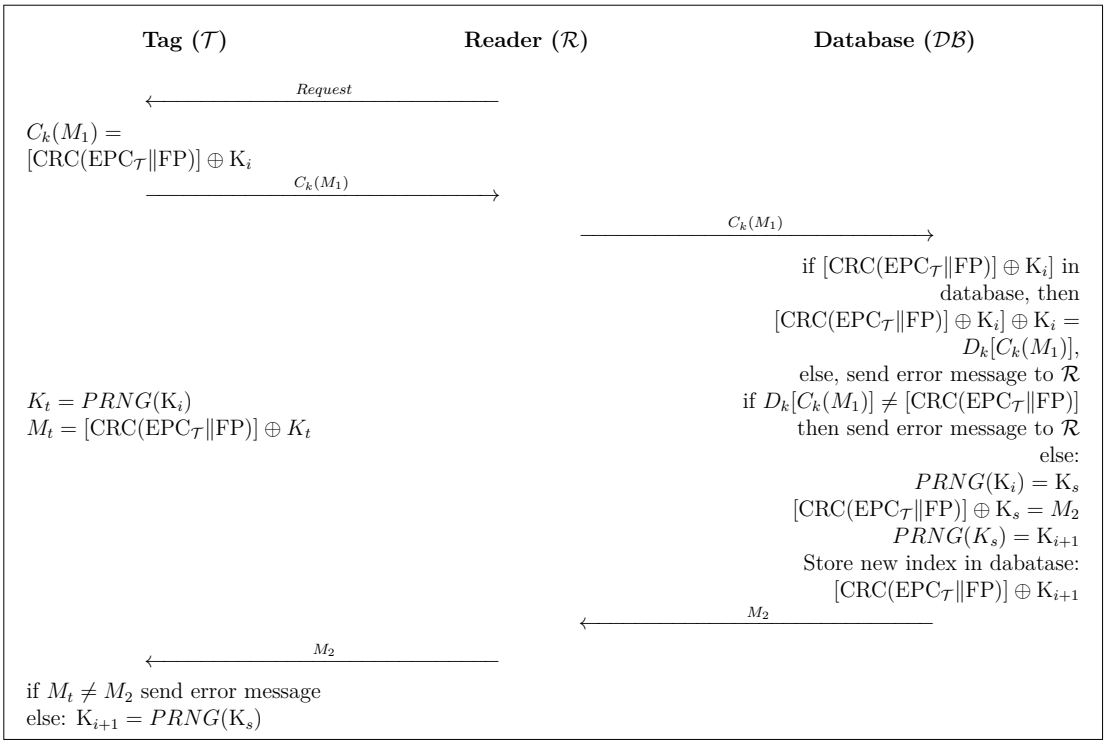


Figure 2.2: Fingerprint-Based Mutual Authentication Protocol [93].

Protocol	Replay Attack	DoS Attack	Cloning Attack	Forward Attack	EPC Compliant
Khor *et al.*	◯	◯	◯	◯	◯
Our Attack	x	x	x	x	◯

Notation: ◯: Satisfied x: Vulnerable

Table 2.2: Security Properties

2.4.1 Full Disclosure Attack

In the fingerprint protocol, and adversary $\mathcal{A}$ can eavesdrop all messages transmitted over the insecure radio channel and exploit the fact that the *PRNG* outputs 16-bit values to be compliant with EPC-C1G2 standard. Taking advantage of this, the private information stored on tags and the server can be compromised. The particular steps of the proposed attack are described below:

1. $\mathcal{A}$ eavesdrops one session of the authentication protocol and picks the messages $C_k(M_1)$ and M_2 off the radio channel:

$$C_k(M_1) = [CRC(\mathrm{EPC}_\mathcal{T} \oplus FP)] \oplus \mathrm{K}_i \quad (2.1)$$

$$M_2 = [CRC(\mathrm{EPC}_\mathcal{T} \oplus FP)] \oplus K_s \quad (2.2)$$

   where

$$K_s = PRNG(\mathrm{K}_i) \quad (2.3)$$

2. Taken into account that the length of CRC is 16 bits, then $\mathcal{A}$ executes a loop from $i = 0$ to $i = 2^{16} - 1$ doing the next computations and checks:

- The value of $CRC(\mathrm{EPC}_{\mathcal{T}} \oplus FP)$ is replaced to i. Then $\widehat{\mathrm{K}_i}$ and $\widehat{M_2}$ are calculated:

$$\widehat{\mathrm{K}_i} = C_k(M1) \oplus i \tag{2.4}$$
$$\widehat{M_2} = i \oplus PNRG(\widehat{\mathrm{K}_i}) \tag{2.5}$$

- At this point, if $\widehat{M_2}$ is equal to M_2, then i and $\widehat{\mathrm{K}_i}$ are returned. Both values are respectively $CRC(\mathrm{EPC}_{\mathcal{T}} \oplus FP)$ and K_i:

$$CRC(\mathrm{EPC}_{\mathcal{T}} \oplus FP) = i \tag{2.6}$$
$$\mathrm{K}_i = \widehat{\mathrm{K}_i} \tag{2.7}$$

Therefore the adversary is able to compromise the private information that the protocol attempts to protect. The probability of success of the given attack is one with a complexity of eavesdropping one session and on-average 2^{15} off-line evaluation of $PRNG$ and some XOR computations.

In the just presented attack, we assume that the adversary can eavesdrop on both forward channel (reader-to-tag) and backward channel (tag-to-reader). Nevertheless, we can assume a much more restrictive condition and consider that $\mathcal{A}$ eavesdrops only on the forward-channel — this is the more restrictive scenario possible taken into account that the radio channel is used. Similarly to the previous attack, $\mathcal{A}$ can disclose private information by eavesdropping on two consecutive protocol sessions and doing some computations. First, $\mathcal{A}$ captures M_2 values:

$$M_2(m) = [CRC(\mathrm{EPC}_{\mathcal{T}} \oplus FP)] \oplus K_s \tag{2.8}$$
$$M_2(m+1) = [CRC(\mathrm{EPC}_{\mathcal{T}} \oplus FP)] \oplus K'_s \tag{2.9}$$

where

$$K'_s = PRNG(K_{i+1}) = PRNG^2(K_s) \tag{2.10}$$

As we previously showed, $\mathcal{A}$ executes an off-line search from $i = 0$ to $i = 2^{16} - 1$ while she does the following computations until a match is found:

$$C = M_2(m) \oplus M_2 \tag{2.11}$$
$$C \stackrel{?}{=} i \oplus PRNG^2(i) \tag{2.12}$$

Finally, $\mathcal{A}$ reveals the session key ($K_s = i$) and the identifier ($CRC(\mathrm{EPC}_{\mathcal{T}} \oplus FP) = M_2(m) \oplus i$) of the target tag. The probability of being successful is one with a complexity of eavesdropping two consecutive sessions and performing on-average 2^{15} off-line evaluations of $PRNG$ function and some XOR computations.

Although the two presented attacks ruin all security objectives of Khor *et al.*'s protocol, we use other strategies against the protocol aiming to show additional weak points of this protocol.

2.4.2 Tag Impersonation

Relay attack is a kind of physical attack where an adversary $\mathcal{A}$ acts as a man-in-the-middle. This attack is as easy as place an illegitimate device between an honest RFID tag and a reader. With this new device, $\mathcal{A}$ is able to intercept, copy, and modify any of messages transmitted between the legitimate tag and reader. Both mentioned devices are fooled into thinking that they are communicating directly with each other when they really are not ([117]).

Replay attack is a kind of multilayer attack where the adversary $\mathcal{A}$ copies valid replies of the communication channel and broadcasts them at a later time to one or more participants in order to get some benefit ([117]).

The authors claim that replay attacks are prevented due to the value transmitted for each session is different. Nevertheless, $\mathcal{A}$ can exploit the fact that the tag only updates its secret key after a successful authentication. More precisely, the attack is divided into two phases:

1. Relay Attack. Let assume $\mathcal{A}$ acts as a man-in-the-middle and an authentication session is executed. $\mathcal{A}$ copies $C_k(M_1)$ value and forwards it to the reader-server. Once M_2 is received, $\mathcal{A}$ alters its content (*i.e.*, flipping one bit) and sends it to the tag. As consequence of the invalid M_2 message, the honest tag sends and error message and $\mathcal{A}$ simply passes it to the reader-server. That is, there is neither key updating in the tag nor in the server (*i.e.*, $K_{i+1} = \mathrm{K}_i$).
2. Replay Attack. Let assume $\mathcal{A}$ copies $C_k(M_1)$ on a counterfeit tag $\widehat{\mathcal{T}}$. This tag forwards this value after the reception of a request message. Once the validity of this message is checked, the server forwards M_2 which is received by $\widehat{\mathcal{T}}$. $\widehat{\mathcal{T}}$ simulates the incorrect reception of M_2 and sends back an error message. The objective of this last error message preventing the key update mechanism is that $\widehat{\mathcal{T}}$ can pass the server authentication in the next session.

So after executing once the relay-attack (Step 2 Replay Attack), a counterfeit tag can supplant indefinitely a legitimate tag just by eavesdropping the message $C_k(M_1)$ previously captured and replying an error message. The probability of success is one and it only requires a man-in-the-middle attack (Step 1 Relay Attack) during a legitimate authentication session.

2.4.3 De-synchronization and DoS Attacks

De-synchronization attack is a kind of multilayer attack. In the RFID context, this kind of attack is often combated by storing the old and new values of the updated variables in the back-end database. Therefore, in a de-synchronization attack the adversary aims to disrupt the key update leaving the tag and reader in a desynchronized state and avoiding future tag's authentication.

In [93] the authors do not use any mechanism for recovering from desynchronized states. Nevertheless, an adversary can de-synchronize a tag and a reader due to both entities only stored the current key. Let assume $\mathcal{A}$ acts as a man-in-the-middle and an authentication session is executed:

1. $\mathcal{A}$ forwards $C_k(M_1)$ to the reader-server. Similarly, it passes M_2 message to the tag.

2. $\mathcal{A}$ simulates the incorrect reception of M_2 and sends and error message to the reader-server.
3. Finally, the tag updates its session key while the back-end server does not update its session key as consequence of receiving the error message:

$$\begin{aligned} K_{i+1} &= PRNG(K_t) \quad \text{(Tag)} \\ K_{i+1} &= PRNG(\mathrm{K}_i) \quad \text{(Reader-Server)} \end{aligned}$$

Therefore, in the next authentication (tag identification), the tag and the database will be desynchronized because both have different keys which makes infeasible future authentications of that tag. The probability of success is one and it only requires a man-in-the-middle attack passing messages and sending an error message during a legitimate authentication session.

2.4.4 Traceability Attack

Privacy (data and location) is one of the most important risk linked to RFID technology. Traceability attacks can be done even if a tag only transmits a static identifier. If a link can be established by $\mathcal{A}$ between the tag and her holder then that person is going to be tracked wherever she goes. For that link it is not necessary to get the entire tag's ID, only with some constant value is enough to track a tag.

We follow the untraceability model proposed by Juels and Weis and later formalized by Phan ([44, 87]). $\mathcal{A}$ performs the following steps:

Phase 1 (Learning) $\mathcal{A}$ sends an Execute($\mathcal{R}$, $\mathcal{T}$, i) query. This phase models a passive attacker. $\mathcal{A}$ eavesdrops on the channel at the i-th session, and gets read access to the exchanged messages between $\mathcal{R}$ and $\mathcal{T}$. More precisely, $\mathcal{A}$ acquires the encrypted message sent by $\mathcal{T}$:

$$Z_1 = C_k(M_1)^{\mathcal{T}_0} = [CRC(\mathrm{EPC}_{\mathcal{T}_0} \oplus FP_{\mathcal{T}_0})] \oplus \mathrm{K}_i^{\mathcal{T}_0}\} \tag{2.13}$$

Then, $\mathcal{A}$ sends a Send($\mathcal{T}$, $\mathcal{R}$, i, M_2') query. This model an active attack (relay attack) by allowing the adversary $\mathcal{A}$ to impersonate $\mathcal{R}$ in protocol session i-th, and send a M_2' message to $\mathcal{T}$. That is, the adversary receives M_2 from the reader, alters randomly its content (*e.g.*, flipping one bit) and sends M_2' to $\mathcal{T}$. As consequence that M_2' is incorrect, the tag sends an error message to the server. Therefore, the tag and server do not update its session keys (see Step 1 in subsection 2.4.2):

$$\begin{aligned} K_{i+1} &= \mathrm{K}_i \quad \text{(Tag)} \\ K_{i+1} &= \mathrm{K}_i \quad \text{(Reader-Server)} \end{aligned} \tag{2.14}$$

Phase 2 (Challenge) $\mathcal{A}$ chooses two fresh tags whose associated identifiers are the tuple $\{\mathrm{EPC}_{\mathcal{T}_0}, FP_{\mathcal{T}_0}\}$ and $\{\mathrm{EPC}_{\mathcal{T}_1}, FP_{\mathcal{T}_1}\}$ respectively. When this query is invoked in session $i+1$-th, a random bit is generated $b \in \{0,1\}$. As result, $C_k(M_1)^{\mathcal{T}_b}$ ciphered token is given depending on the chosen random bit:

$$Z_2 = \begin{cases} C_k(M_1)^{\mathcal{T}_0} = [CRC(\mathrm{EPC}_{\mathcal{T}_0} \oplus FP_{\mathcal{T}_0})] \oplus K_i^{\mathcal{T}_0}, & \text{if } b = 0 \\ C_k(M_1)^{\mathcal{T}_1} = [CRC(\mathrm{EPC}_{\mathcal{T}_1} \oplus FP_{\mathcal{T}_1})] \oplus K_{i+1}^{\mathcal{T}_1}, & \text{if } b = 1 \end{cases} \tag{2.15}$$

Phase 3 (Guessing) A outputs a bit d ($d \in \{0,1\}$) as her guess of the value b. In particular, we propose the following simple decision rule to obtain value d:

$$d = \begin{cases} 0 & \text{if } Z_1 == Z_2 \\ 1 & \text{if } Z_1 \neq Z_2 \end{cases} \tag{2.16}$$

Summarizing, we can track tags exploiting the fact that we can deceive tag and server to use the same (constant) key permanently. On the other hand, the protocol does not use any random number to guarantee the freshness of the messages linked to each session. Formally and according to [44] and [87], the advantage of $\mathcal{A}$ in distinguishing whether the adversary interacts with $\mathcal{T}_0$ or $\mathcal{T}_1$ is:

$$Adv_{\mathcal{A}}^{UNT}(t,1) = |Pr[d == b] - \frac{1}{2}| = |1 - \frac{1}{2}| = \frac{1}{2} \tag{2.17}$$

So the advantage is maximum and an adversary tracks a tag meeting with success 100% of her attempts.

2.5 Improved protocol: Fingerprint$^+$

In this section we present an improved version of the protocol analysed in the previous sections. To avoid security pitfalls the proposed scheme is based on well-known security standards and tailored to the particular features of an EPC friendly authentication protocol. On one hand the protocol conforms the requirements of the EPC-C1G2 standard and tags only support a *PRNG* and bitwise operations for security purposes. Since the security-level of the protocol resides on the *PRNG* function, we recommend the usage of an output length of at least 64 bits note that NIST recommendation is even more restrictive [1]. On the other hand, and instead of designing a protocol from scratch, our proposed protocol is highly inspired on ISO/IEC 9798 Part 2. In this regulation four protocols are specified to provide entity authentication and two other ones provide also key establishment. More precisely, Fingerprint$^+$ protocol is based on the ISO/IEC 9798-2 three-pass mutual authentication scheme.

In Figure 2.3 we sketch the messages exchanged between the tag and the back-end server. In the initialization phase the server stores four values of each tag ($\text{EPC}_{\mathcal{T}}$, FP, $DATA$, K_i). Correspondingly the tag stores three values ($\text{EPC}_{\mathcal{T}}$, FP, K_i), which are required for the authentication process. In the authentication phase the reader generates a random number $N_{\mathcal{R}}$ and sends this value together a request message to the tag. Once the request is received, the tag generates two random numbers, named in the scheme as the session nonce N_S and tag nonce $N_{\mathcal{T}}$. Then, the nonces, an anonymous identifier ($A_I = PRNG(N_S, N_{\mathcal{T}}, \text{EPC}, FP)$) and an authentication token ($A_{T_{\mathcal{T}}} = PRNG(\text{K}_i, N_S, N_{\mathcal{R}})$) are sent back to the reader and forwarded to the server. At the server side, the tag is firstly identified by the anonymous identifier (pseudonym) and then the authentication token is verified. If any of the tags belonging to the tag population managed by the server is identified or the authentication process fails, an error message is sent back to the reader. Otherwise, the tag is correctly identified and successfully authenticated. At this point the server generates

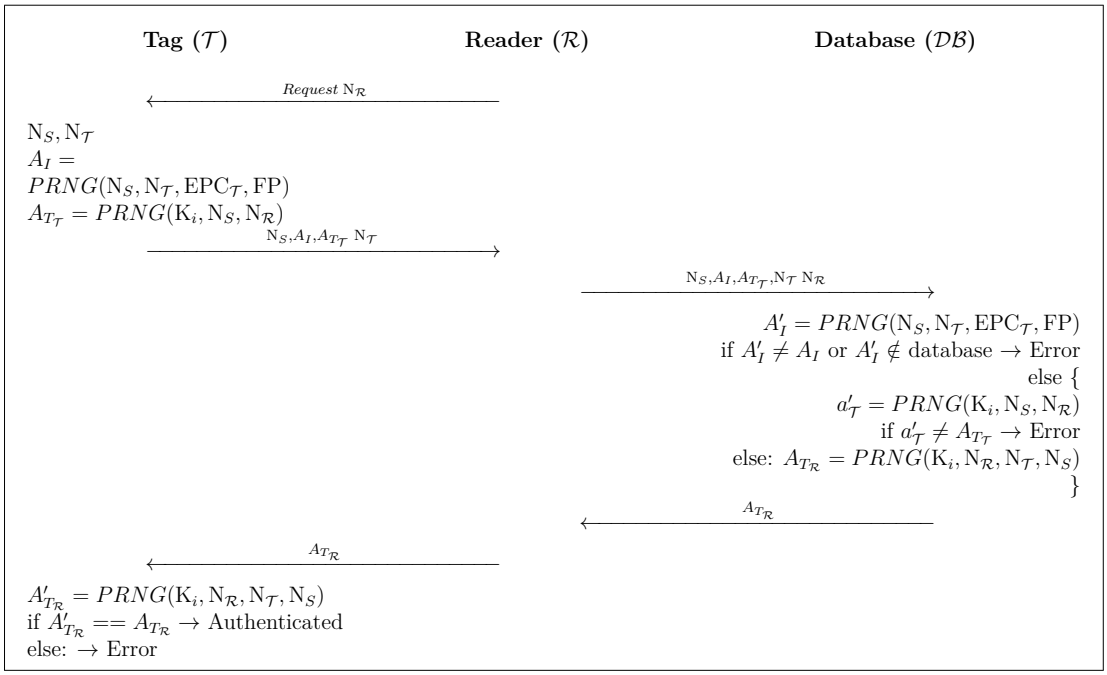


Figure 2.3: Fingerprint$^+$ Mutual Authentication Protocol

an authentication token $PRNG(K_i, N_{\mathcal{R}}, N_{\mathcal{T}}, N_S)$ and forwards it to the tag through the reader. The tag computes a local version of this token and compares it with the received one. If both are equal, the mutual authentication concludes successfully. If not, the tag sends back an error message to the server.

The security of the proposed protocol resides on the security of a well-known and internationally recognized standard. In particular the security of ISO/IEC 9798-2 three pass mutual authentication has been deeply scrutinized and no-attacks are known. Fingerprint$^+$ has been designed conforming this standard in order to inherit its security properties. In relation to its predecessor, which is not based in any security standard, we have overcome all of its security deficiencies. We have avoided the use of CRCs for security purposes since this sort of functions are linear. Our scheme is based on the usage of a *PRNG* other primitives could have been used but the EPC standard sets this restriction. To guarantee the freshness of the messages and combat replay attacks three nonces are involved in each session and both entities generate at least one of them. On the other hand, our protocol does not need of a key updating scheme as stated in ISO 9798-2 standard and this fact discards de-synchronization attacks. Finally we have guaranteed the privacy of the identifiers (EPC and FP) by the usage of pseudonyms.

2.5.1 Performance Analysis

In our protocol we have introduced two slight changes (*i.e.*, the use of a *PRNG* function and pseudonyms) in comparison to the original protocol [93]. The rest of the protocol (*e.g.*, protocol steps) is preserved without modifications in order to guarantee the same performance as the original one and to keep in compliance with the EPC standard. In addition we have analysed the performance of our proposal in

terms of computational and communication costs, and storage requirements, which are the common properties evaluated in other proposals. The details are given below:

- **Computational cost**: Fingerprint$^+$ only requires simple *PRNG* calculations. Computational cost is negligible on both reader and server side. On tags these operations are very low-cost and can be efficiently implemented on-board of EPC tag's hardware even with 96-bits length which is the length commonly assumed on EPC standard [53].
- **Storage requirements**: Each tag stores two static identifiers (EPC and FP) and the key K_i. Furthermore three random numbers are used in the authentication phase: N_S, $N_{\mathcal{T}}$, $N_{\mathcal{R}}$. As said before, a 96-bit length is assumed for all elements in accordance with EPC standard [53]. Because EPC, FP and K_i are static values, these could be stored in ROM ($96 \times 3 = 288$ bits). The remaining values ($96 \times 3 = 288$ bits) are stored in the rewritable memory.
- **Communication cost**: In the communication phase, 6 messages and a "Request" message are sent over the channel (Reader-Tag) in order to authenticate mutually both parties. Considering 2 bytes for the "Request" message, a total amount of 74 bytes are passed over the channel.

2.5.2 Security Analysis of Improved Protocol: Fingerprint$^+$

There are two main ways to prove the security of cryptographic authentication protocols: informal and formal methods. An informal method of security correctness proof of a cryptographic protocol relays on the heuristic opinions by security experts to draw a conclusion. On the other hand, a formal method relies on mathematical rules and frameworks. In this section we first show that the advantage of any adversary to mount an attack against Fingerprint$^+$ is negligible, see Theorem 1. Next, we formally show that Fingerprint$^+$ is immune against the attacks presented in this chapter and also against other known active and passive attacks. Therefore we can claim that our improved protocol offers a higher security level than its predecessors.

Theorem 1. *Assuming that for each fresh query, the used* $PRNG : \{0,1\}^* \rightarrow \{0,1\}^n$ *returns a uniformly distributed random value within its range, the adversary's advantage to mount a successful attack after* q *sessions of the Fingerprint*$^+$*'s protocol, is upper bounded by* $\frac{3q^2}{2^n}$.

Proof. We first clarify that we only consider non trivial adversaries that need to like transferred values over the protocol or to output a message to be accepted by a party of the protocol. Hence, we rule out any adversary who does not analyse the details of the transferred messages, e.g., an adversary who just blocks the transferred messages.

Public messages in a given session of Fingerprint$^+$ are as below:

$$
\begin{aligned}
M1 &: \mathcal{R}_i \rightarrow \mathcal{T}_i : Request, N_{\mathcal{R}} \\
M2 &: \mathcal{T}_i \rightarrow \mathcal{R}_i : N_S, PRNG(N_S, N_{\mathcal{T}}, \mathrm{EPC}_{\mathcal{T}_i}, FP), \\
&\qquad\qquad PRNG(K_i, N_S, N_{\mathcal{R}}), N_{\mathcal{T}} \\
M3 &: \mathcal{R}_i \rightarrow S : N_S, N_{\mathcal{R}}, N_{\mathcal{T}}, \\
&\qquad\qquad PRNG(N_S, N_{\mathcal{T}}, \mathrm{EPC}_{\mathcal{T}_i}, FP), PRNG(K_i, N_S, N_{\mathcal{R}}) \\
M4 &: S \rightarrow \mathcal{R}_i : PRNG(K_i, N_{\mathcal{R}}, N_{\mathcal{T}}, N_S) \\
M5 &: \mathcal{R}_i \rightarrow \mathcal{T}_i : PRNG(K_i, N_{\mathcal{R}}, N_{\mathcal{T}}, N_S)
\end{aligned}
$$

Hence, we can consider three different following categorization for adversaries according to its attack:

1. Passive adversaries who eavesdrop public messages - Such an adversary has no control over $N_{\mathcal{R}}$, N_S and $N_{\mathcal{T}}$. Hence, for such an adversary $PRNG(N_S, N_{\mathcal{T}}, \mathrm{EPC}_{\mathcal{T}_i}, FP)$, $PRNG(K_i, N_S, N_{\mathcal{R}})$ and $PRNG(K_i, N_{\mathcal{R}}, N_{\mathcal{T}}, N_S)$ are uniformly randomized for any session, as long as both the reader and the tag have not used a repeated set of random values. Since any message is at leased randomized by two random values, the adversary's advantage to link any two transferred messages is upper bounded by $\frac{1}{2^{2n}}$ and the adversary's success probability after q sessions is upper bounded by $\frac{3q^2}{2^{2n}}$
2. Active adversaries who control public messages from the reader to the tag - Such an adversary can control $N_{\mathcal{R}}$, however N_S and $N_{\mathcal{T}}$ are out of her control. Hence, for such an adversary $PRNG(N_S, N_{\mathcal{T}}, \mathrm{EPC}_{\mathcal{T}_i}, FP)$, $PRNG(K_i, N_S, N_{\mathcal{R}})$ and $PRNG(K_i, N_{\mathcal{R}}, N_{\mathcal{T}}, N_S)$ are uniformly randomized for any session, as long as the tag has not used a repeated random value. Since any message is at leased randomized by a random value generated by the tag (message which is not under adversary's control), the adversary's advantage to link any two transferred messages or to output a modified message which is accepted by the tag is upper bounded by $\frac{1}{2^n}$. Hence, the adversary's success probability after q sessions is upper bounded by $\frac{3q^2}{2^n}$.
3. Active adversaries who control public message from the tag to the reader - Such an adversary can control N_S and $N_{\mathcal{T}}$, however $N_{\mathcal{R}}$ is out of her control. Hence, for such an adversary $PRNG(N_S, N_{\mathcal{T}}, \mathrm{EPC}_{\mathcal{T}_i}, FP)$, $PRNG(K_i, N_S, N_{\mathcal{R}})$ and $PRNG(K_i, N_{\mathcal{R}}, N_{\mathcal{T}}, N_S)$ are uniformly randomized for any session, as long as the reader has not used the same $N_{\mathcal{R}}$ in two different sessions. Since any message is randomized by $N_{\mathcal{R}}$ (message which is not under adversary's control), the adversary's advantage to link any two transferred messages or to output a modified message which is accepted by the reader is upper bounded by $\frac{1}{2^n}$. Hence, the adversary's success probability after q sessions is upper bounded by $\frac{3q^2}{2^n}$.

Therefore we can conclude that for any active or passive adversary, that needs either to link messages or to output a correct message, the success probability after q attempt is upper bounded by $\frac{3q^2}{2^n}$. On the other hand, in any conventional attack for RFID systems, e.g., tag/reader impersonation and traceability, the adversary should

either links transferred messages in different sessions or outputs a valid message that is accepted by a protocol party. Thus the adversary's advantage to mount an attack against Fingerprint$^+$ is upper bounded by $\frac{3q^2}{2^n}$.

It must be noted that an adversary could change a message and send it to the reader/tag to be authenticated by that party. However, for example if the adversary modifies $PRNG(K_i, N_{\mathcal{R}}, N_{\mathcal{T}}, N_S)$ in the last step to the tag to any desired value, the value will be authenticated by the tag with the probability of $\frac{1}{2^n}$, which is far lower than the considered advantage for the adversary. Almost a similar argument can be presented for an adversary who changes the messages to the reader. Hence, $\frac{3q^2}{2^n}$ is the upper bound of the adversary's advantage to mount an attack. □

2.5.2.1 Formal Security Analysis

A formal method is a technique to analyse the security of a cryptographic protocol which describes the protocol properties based on mathematics and logic. That is, the target protocol and its features are modelled based on algebra and logic. Several logic tools exist to prove the security correctness of a cryptographic authentication protocol, *e.g.*, BAN logic [35], GNY logic [65], AVISPA tool [10] and Proverif tool [26].

In this chapter, we use BAN logic to prove the security correctness of Fingerprint$^+$. We formally show that after one run of Fingerprint$^+$ the tag, the reader and the server believe the received messages are from the expected sender and these messages are fresh. Hence, they can be authenticated by each other properly.

To prove the security of a protocol formally with BAN logic the following four steps [35] should be followed:

- The messages and the actions of the protocol parties should be represented by mathematical relations.
- The messages and the actions of the protocol parties should be converted into BAN logic formulas and dropping the plain text messages from protocol messages. In this step, the resulting protocol messages are called idealized messages.
- The protocol initial assumptions and security goals should be explained as BAN logic formulas.
- Finally the protocol security goals should be deduced. In this step, using BAN logic rules it is evaluated whether protocol security goals are satisfied or not.

In bellow, $\mathcal{R}_i$, $\mathcal{T}_i$ and S symbolize the reader, the tag and the database server respectively. We also show BAN logic notations and rules which are used in our proof in Table 2.1.

Mathematical stating the protocol's messages

At the first step we mathematically, similar to Theorem 1, represent the messages of Fingerprint$^+$ as below:

$$
\begin{aligned}
M1 &: \mathcal{R}_i \rightarrow \mathcal{T}_i : Request, N_{\mathcal{R}} \\
M2 &: \mathcal{T}_i \rightarrow \mathcal{R}_i : N_S, PRNG(N_S, N_{\mathcal{T}}, \mathrm{EPC}_{\mathcal{T}_i}, FP), \\
&\qquad PRNG(K_i, N_S, N_{\mathcal{R}}), N_{\mathcal{T}} \\
M3 &: \mathcal{R}_i \rightarrow S : N_S, N_{\mathcal{R}}, N_{\mathcal{T}}, \\
&\qquad PRNG(N_S, N_{\mathcal{T}}, \mathrm{EPC}_{\mathcal{T}_i}, FP), PRNG(K_i, N_S, N_{\mathcal{R}}) \\
M4 &: S \rightarrow \mathcal{R}_i : PRNG(K_i, N_{\mathcal{R}}, N_{\mathcal{T}}, N_S) \\
M5 &: \mathcal{R}_i \rightarrow \mathcal{T}_i : PRNG(K_i, N_{\mathcal{R}}, N_{\mathcal{T}}, N_S)
\end{aligned}
$$

Converting the protocol messages into idealized form based on BAN logic formulas

In this stage, we transform each Fingerprint$^+$ś message into an idealized message, i.e., plaintexts are omitted from protocol messages and only encrypted message contents are relevant to this step. We also use BAN logic notations for representing these idealized messages as follows:

$$
\begin{aligned}
IM1 &: \mathcal{R}_i \triangleleft \{N_S, N_{\mathcal{T}}, FP\}_{\mathrm{EPC}_{\mathcal{T}_i}} \\
IM2 &: \mathcal{R}_i \triangleleft \{N_S, N_{\mathcal{R}}\}_{K_i} \\
IM3 &: S \triangleleft \{N_S, N_{\mathcal{T}}, FP\}_{\mathrm{EPC}_{\mathcal{T}_i}} \\
IM4 &: S \triangleleft \{N_S, N_{\mathcal{R}}\}_{K_i} \\
IM5 &: \mathcal{R}_i \triangleleft \{N_{\mathcal{R}}, N_{\mathcal{T}}, N_S\}_{\mathrm{K}_i} \\
IM6 &: \mathcal{T}_i \triangleleft \{N_{\mathcal{R}}, N_{\mathcal{T}}, N_S\}_{\mathrm{K}_i}
\end{aligned}
$$

Representing initial assumptions and security goals as BAN logic formulas

The explicit assumptions of our proposed protocol are shown below:

$$
\begin{aligned}
A1 &: \mathcal{T}_i| \equiv S \overset{\mathrm{K}_i}{\longleftrightarrow} \mathcal{T}_i \\
A2 &: S| \equiv \mathcal{T}_i \overset{\mathrm{K}_i}{\longleftrightarrow} S \\
A3 &: \mathcal{T}_i| \equiv S \overset{\mathrm{EPC}_{\mathcal{T}_i}}{\longleftrightarrow} \mathcal{T}_i \\
A4 &: S| \equiv \mathcal{T}_i \overset{\mathrm{EPC}_{\mathcal{T}_i}}{\longleftrightarrow} S \\
A5 &: \mathcal{T}_i| \equiv S \overset{FP}{\longleftrightarrow} \mathcal{T}_i \\
A6 &: S| \equiv \mathcal{T}_i \overset{FP}{\longleftrightarrow} S \\
A7 &: \mathcal{T}_i| \equiv \#(N_S) \\
A8 &: \mathcal{T}_i| \equiv \#(N_{\mathcal{T}}) \\
A9 &: \mathcal{R}_i| \equiv \#(N_{\mathcal{R}})
\end{aligned}
$$

Assumptions $A1$ to $A6$ are related to secrets which are shared between protocol's parties. Assumptions $A7$ to $A9$ are linked with freshness of random numbers which are generated by the tag and the reader, respectively.

The goals of our Fingerprint$^+$ are as below:

$$G_1 : S| \equiv \mathcal{T}_i| \sim FP$$
$$G_2 : S| \equiv \mathcal{T}_i| \sim N_S$$
$$G_3 : \mathcal{T}_i| \equiv S| \sim N_{\mathcal{R}}$$

G_1 means that the server believes the tag $\mathcal{T}_i$ has sent fingerprint FP. This indicates that the adversary has not changed this fingerprint, which was generated by the tag and sent through the reader to the server. Therefore, the adversary cannot apply any attack on the protocol that requires any change on this fingerprint.

G_2 means that the server believes the tag has sent N_S. This indicates that the adversary has not changed this data which was generated by the tag and sent through the reader to the server.

G_3 means that the tag believes the server has sent $N_{\mathcal{R}}$. This indicates that the adversary has not changed this data which was generated by the reader and sent to the tag.

Deducing the protocol security goals

BAN logic rules are expressed as fractional forms [35] which if its numerator expressions are correct then it can be concluded that the denominator expressions are also correct. In this step we combine idealized messages and the assumptions to construct numerator expressions of BAN logic rules. These numerators are used to prove the correctness of the denominator expressions that are corresponding to the security goals. We show these deductions as below:

If we consider $IM3$ idealized message, i.e., $S \triangleleft \{N_S, N_{\mathcal{T}}, FP\}_{\mathrm{EPC}_{\mathcal{T}_i}}$ with $A4$ assumption, i.e., $S| \equiv \mathcal{T}_i \overset{\mathrm{EPC}_{\mathcal{T}_i}}{\longleftrightarrow} S$, it can be easily seen the numerator of BAN logic $P1$ rule, i.e., $\frac{P| \equiv P \overset{K}{\longleftrightarrow} Q, P \triangleleft \{X\}_K}{P| \equiv Q| \sim X}$ is constructed and thus we can deduce that the denominator is also correct. It can be seen as follows:

$$D1 : IM3, A4, P1 \Rightarrow S| \equiv \mathcal{T}_i| \sim \{N_S, N_{\mathcal{T}}, FP\}$$

Similarly if we consider the previous results, i.e., $D1 : S| \equiv T_i| \sim \{N_S, N_{\mathcal{T}}, FP\}$, it can be easily seen the numerator of BAN logic $P2 : \frac{P| \equiv Q| \sim \{X,Y\}}{P| \equiv Q| \sim \{X\}}$ rule is constructed and thus we can deduce the denominator is also correct as shown below:

$$D2 : D1, P2 \Rightarrow S| \equiv \mathcal{T}_i| \sim FP$$

Next, consider $IM4$ idealized message, i.e., $S \triangleleft \{N_S, N_{\mathcal{R}}\}_{K_i}$ with $A2$ assumption, i.e.,$S| \equiv \mathcal{T}_i \overset{\mathrm{K}_i}{\longleftrightarrow} S$, it can be easily seen the numerator of BAN logic $P1$ rule, i.e.,

$\frac{P|\equiv P\overset{K}{\longleftrightarrow}Q,P\triangleleft\{X\}_K}{P|\equiv Q|\sim X}$ is constructed and thus we can deduce the denominator is also correct. It can be seen as follows:

$$D3 : IM4, A2, P1 \Rightarrow S|\equiv \mathcal{T}_i|\sim\{N_S, N_{\mathcal{R}}\}$$

In addition, if we consider the previous results, i.e., $D3 : S|\equiv \mathcal{T}_i|\sim\{N_S,N_{\mathcal{R}}\}$, it can be easily seen the numerator of BAN logic $P2 : \frac{P|\equiv Q\sim\{X,Y\}}{P|\equiv Q|\sim\{X\}}$ rule is constructed and thus we can deduce the denominator is also correct as shown below:

$$D4 : D3, P2 \Rightarrow S|\equiv \mathcal{T}_i|\sim N_S$$

Now, if we consider $IM6$ idealized message, i.e., $\mathcal{T}_i\triangleleft\{N_{\mathcal{R}},N_{\mathcal{T}},N_S\}_{\mathrm{K}_i}$ with $A1$ assumption, i.e., $\mathcal{T}_i|\equiv S\overset{\mathrm{K}_i}{\longleftrightarrow}\mathcal{T}_i$, it can be easily seen the numerator of BAN logic $P1$ rule, i.e., $\frac{P|\equiv P\overset{K}{\longleftrightarrow}Q,P\triangleleft\{X\}_K}{P|\equiv Q|\sim X}$ is constructed and thus we can deduce the denominator is also correct. It can be seen as follows:

$$D5 : IM6, A1, P1 \Rightarrow \mathcal{T}_i|\equiv S|\sim\{N_{\mathcal{R}}, N_{\mathcal{T}}, N_S\}$$

If we consider $D5 : \mathcal{T}_i|\equiv S|\sim\{N_{\mathcal{R}}, N_{\mathcal{T}}, N_S\}$, it can be easily seen the numerator of BAN logic $P2 : \frac{P|\equiv Q\sim\{X,Y\}}{P|\equiv Q|\sim\{X\}}$ rule is constructed and thus we can deduce the denominator is also correct as shown below:

$$D6 : D5, P2 \Rightarrow \mathcal{T}_i|\equiv S|\sim N_{\mathcal{R}}$$

Finally, it can be seen that $D_2 == G_1$, $D_4 == G_2$ and $D_6 == G_3$ and then our proposed protocol security goals G_1, G_2 and G_3 are satisfied.

2.6 Conclusions

In this chapter we show that fingerprint-based authentication protocol proposed in [93] by Jing Huey Khor *et al.* is completely insecure. An attacker, equipped with a domestic PC, can execute a full disclosure attack in only a few minutes. On the other hand, there is not any source of freshness in any of the messages of the protocol, strategy that is often needed to combat replay attacks. Furthermore, de-synchronization of the protocol is simple because the server and the tag only keep the current session key. In fact, there is not any mechanism to recover from a previous state when an incorrect message is received due to errors in the channel

or manipulations by an adversary. Therefore, this chapter ruins all the security objectives that the protocol aims to offer.

To avoid that protocols are almost immediately cryptanalysed after its proposal, the use of well-known security approaches is recommended. In our particular case we present Fingerprint$^+$ protocol and then formally prove its security. The improved protocol is based on ISO/IEC 9798-2 and EPC-C1G2 standard equivalently ISO/IEC 18000-6C.

3

Two RFID standard-based security protocols for healthcare environments

3.1 Introduction

RFID is a technology for remote identification using radio waves. An RFID system is composed of tags, readers and a database for access and authentication management procedures. There are three different types of tags according to their source of power. Active tags the most expensive are equipped with a battery and can start a connection with a reader by themselves. Passive tags are the cheapest ones, do not have any on-board source of power and harvest energy from the reader signal. Semi-passive tags lie somewhere in between both classes, as they use their own battery for computations but collect energy from the reader signal for communication purposes.

Tying up RFID technology and healthcare environments has been the focus of much research recently due to the potential benefits that this technology could offer, both in terms of savings in operational costs and as enablers of novel applications [152, 172]. As shown in Table 3.1, the range of healthcare problems where RFID could be successfully applied is significant, in some cases with important benefits. For example, the theft of newborn children is a worldwide problem that has recently made the news. It is claimed that in the last 50 years more than 300,000 newborns were abducted in Spain [112]. Similar cases have been reported in Australia [51], while in the US the National Center for Missing & Exploited Children has published some statistics about this alarming problem [120]. To address this problem, several hospitals in different countries have adopted a new and controversial RFID-based solution [13, 108, 165].

Security and privacy concerns associated with the widespread adoption of RFID systems in healthcare environments have been a major deterrent for the penetration of this technology in key application areas. In the last five years, many works have addressed some of these issues by proposing different schemes that facilitate a secure execution of certain healthcare functions. The majority of such schemes have been soon proved insecure despite the claims made in their original proposals. For example, in 2009 Huang and Ku proposed a grouping proof to guarantee medication safety of inpatients [76]. Soon after it was shown that the scheme was vulnerable to DoS and replay attacks [46]. Chien *et al.* suggested a more secure version, but unfortunately an adversary can still conduct impersonation and replay attacks with

Patient Traceability	[119, 170]
Asset Management	[126, 140]
Medication Administration	[8, 174]
Handling Errors	[37, 129]
Ownership Transfer Procedures	[169, 181]
Efficiency Management	[129, 171]
Cost Savings	[33, 170]

Table 3.1: Some healthcare applications of RFID technology.

a high success probability [133]. In this direction, the IS-RFID system proposed in [133] seems an interesting proposal to combat medication errors, but the system does not guarantee that the proofs cannot be manipulated by the hospital [174], which can be crucial in case of dispute due to malpractice. In 2012, Chen *et al.* [40] proposed a novel RFID-based tamper-resistant prescription access control protocol for different authorized readers. Yet again, the protocol was proved to suffer from impersonation, traceability and de-synchronization attacks [144].

3.1.1 Contributions and Organization

Wu *et al.* have recently proposed a new RFID authentication protocol for healthcare environments [164]. Apart from guaranteeing some essential security properties, the protocol claims to solve the trade-off between location privacy and scalability in healthcare environments. A description of Wu *et al.*'s protocol is provided later in subsection 3.2. In this subsection, we first show that this protocol is vulnerable to a traceability attack that allows an adversary to compromise the location privacy of the tag's holder (*e.g.*, a patient, doctor or nurse). The detailed description and analysis of this attack is provided in subsection 3.3. A brief summary of the ISO/IEC 9798 parts 1 to 6 is presented in subsection 3.4. Subsequently in subsection 3.5 we propose authentication and secure messaging protocols based on established ISO standard and well-known security recommendations. In particular, we tailor an entity authentication protocol from ISO/IEC 9798 Part 2 and a secure messaging protocol from ISO/IEC 11770 Part 2 similar to that used in electronic passports. In addition, we discuss some implementation aspects and suggest specific primitives based on NIST 800-38A, NIST 800-38B, and NIST 800-108 recommendations. Finally, subsection 3.6 concludes the chapter by summarizing our main results.

3.2 Wu *et al.'s* Protocol

Wu *et al.* introduce in [164] a novel authentication protocol to be used in open environments such as academic medical centres or metropolitan and local community hospitals. The authors claim that the proposal solves the trade-off between location privacy and scalability in healthcare environments. Figure 3.1 shows the main steps involved in the scheme using the notation provided by Table 3.2.

The protocol consists of two different phases: setup and execution. In the setup

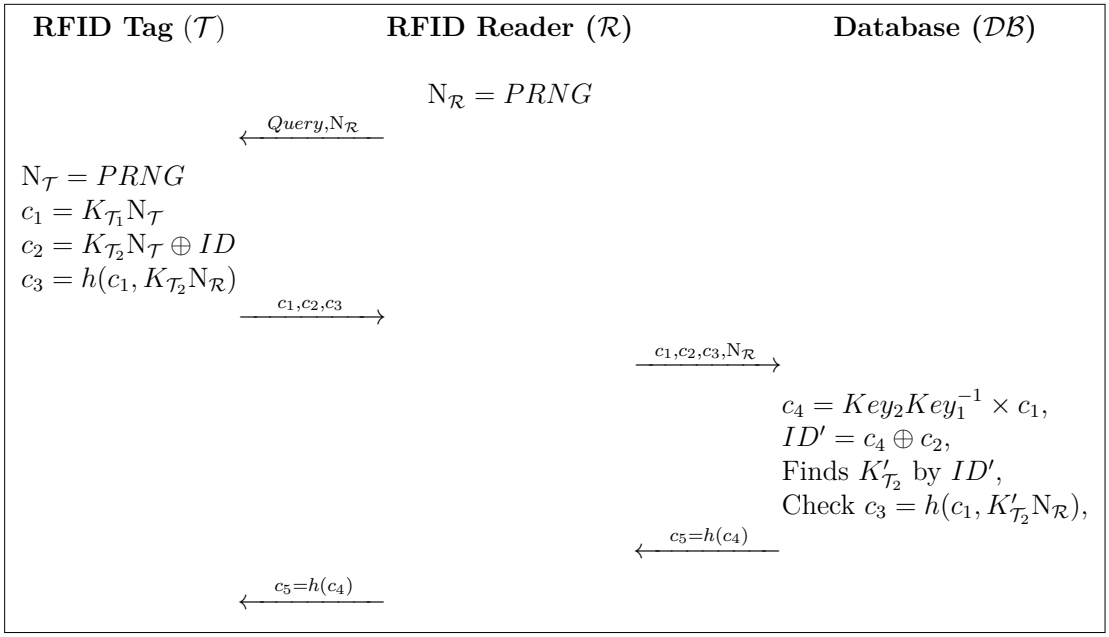


Figure 3.1: Wu *et al.'s* Authentication Protocol [164].

phase, the server generates three $d \times d$ binary matrices (Key_1, Key_2, Key_3), where Key_1 is a nonsingular matrix and Key_3 is a singular one. After that, the server generates two matrices for each tag: $K_{\mathcal{T}_1} = Key_1 Key_3 S_{\mathcal{T}}$ and $K_{\mathcal{T}_2} = Key_2 Key_3 S_{\mathcal{T}}$, where $S_{\mathcal{T}}$ is a random matrix of size $d \times d$. The execution phase of the protocol is described below:

Step 1: The reader ($\mathcal{R}$) sends a query signal and a random value $N_{\mathcal{R}}$ to the tag.

Step 2: The tag ($\mathcal{T}$) generates a random value $N_{\mathcal{T}}$ and computes $c_1 = K_{\mathcal{T}_1} N_{\mathcal{T}}$, $c_2 = K_{\mathcal{T}_2} N_{\mathcal{T}} \oplus ID$, and $c_3 = h(c_1, K_{\mathcal{T}_2} N_{\mathcal{R}})$. Finally, the tag sends c_1, c_2, and c_3 to the reader.

Step 3: $\mathcal{R}$ appends $N_{\mathcal{R}}$ to the received messages c_1, c_2, and c_3 and forwards them to the server.

Step 4: The server computes $c_4 = Key_2 Key_1^{-1} \times c_1$ and recovers the ID by computing $c_4 \oplus c_2$. Then, the server checks if the calculated matrix key $K'_{\mathcal{T}_2}$ matches the received c_3. To do this, a local version of c_3 is computed as $c'_3 = h(c_1, K'_{\mathcal{T}_2} N_{\mathcal{R}})$. If both are equal the reader authenticates the tag; otherwise the server informs the reader to restart the communication or simply reject it.

Step 5: The server computes $c_5 = h(c_4)$ and sends it to the tag.

Step 6: Finally, $\mathcal{T}$ checks if c_5 is equal to $h(K'_{\mathcal{T}_2} N_{\mathcal{T}})$. If so, the tag believes that this message comes from a valid reader (reader authentication).

3.3 Location Attack against Wu *et al.*'s Protocol

In this section, we show that the Wu *et al.*'s protocol fails to preserve the location privacy of a tag's holder. In fact, an adversary $\mathcal{A}$ can execute a successful traceability attack that requires to eavesdrop only a few authentication sessions. The details of the proposed attack are given below.

$K_{\mathcal{T}}$	Secret key of tag $\mathcal{T}$
Key	Secret key of the server
ID	Identification number of the tag
$N_{\mathcal{R}}, N_{\mathcal{T}}$	Nonces chosen by the reader and the tag, respectively
$h(.)$	A hash function
$\oplus$	Bit-wise exclusive OR operation.
A^{-1}	Inverse of matrix A.
AB	Multiplication of matrices A and B

Table 3.2: Notation used in Wu *et al.'s* protocol [164].

Wu *et al.* analyse extensively their protocol to prove that the proposed scheme provides location privacy. They claim that the adversary advantage to trace a given tag after q queries[1] is upper bounded by $\frac{q^2}{2^{l+1}}$, where l is the output length of the hash function used in the protocol. Nevertheless, we show how an active adversary can efficiently trace any given tag in this protocol with an advantage significantly higher than that. The presented attack is based on the following observation, which was missed by the designers:

First Assume that $(A)_i$ denotes the i-th column of matrix A. Let X and X' be random binary matrices of size $d \times d$, and Y and Y' fixed binary matrices of size $d \times r$.

1. If $(X)_i = (X')_j$ and $Y = Y'$, then $(Y \times X)_i = (Y' \times X')_j$ with probability 1.
2. If $(X)_i = (X')_j$ and $Y \neq Y'$, then $(Y \times X)_j = (Y' \times X')_j$ with probability 2^{-d}.

Recall that in Wu *et al.*'s protocol, we have $c_1 = K_{\mathcal{T}_1} N_{\mathcal{T}}$ and $c_2 = K_{\mathcal{T}_2} N_{\mathcal{T}} \oplus ID$, where $K_{\mathcal{T}_1}$ is a nonsingular matrix. Thus, if $(N_{\mathcal{T}})_i = (N'_{\mathcal{T}})_j$ then:

$$(K_{\mathcal{T}_1} N_{\mathcal{T}})_i = (K_{\mathcal{T}_1} N'_{\mathcal{T}})_j$$

and

$$(K_{\mathcal{T}_2} N_{\mathcal{T}} \oplus ID)_i = (K_{\mathcal{T}_2} N'_{\mathcal{T}} \oplus ID)_j$$

Based on the above observation, an adversary $\mathcal{A}$ can perform the following steps to trace a target tag $\mathcal{T}$:

Phase 1 (Learning): $\mathcal{A}$ creates a table Tab with N rows and runs N sessions with the tag $\mathcal{T}$ as follows. At each run $1 \leq j \leq N$:

1. $\mathcal{A}$ sends $N^j_{\mathcal{R}} \in \{0,1\}^l$ to the tag.
2. $\mathcal{T}$ generates a random value $N^j_{\mathcal{T}}$ and computes $c^j_1 = K_{\mathcal{T}_1} N^j_{\mathcal{T}}$, $c^j_2 = K_{\mathcal{T}_2} N^j_{\mathcal{T}} \oplus ID$ and $c^j_3 = h(c^j_1, K_{\mathcal{T}_2} N^j_{\mathcal{R}})$. Finally, $\mathcal{T}$ sends c^j_1, c^j_2, and c^j_3 to $\mathcal{A}$ (since he is acting as a reader).
3. $\mathcal{A}$ stores c^j_1 and c^j_2 in the j-th row of Tab.

Phase 2 (Execution): Given a tag $\mathcal{T}$', the adversary proceeds exactly as in the learning phase, creating a table Tab' with N' columns and running N' sessions with $\mathcal{T}$' as follows. At each run $1 \leq f \leq N$:

[1] In the location-privacy game used in [164] a query represents the hash query of $\mathcal{T}$ or an anonymous query sent to $\mathcal{T}$.

1. $\mathcal{A}$ sends $N_{\mathcal{R}}^f \in \{0,1\}^l$ to the tag.
2. $\mathcal{T}$' generates a random value $N_{\mathcal{T}}^f$ and computes $c_1^f = K_{\mathcal{T}_1} N_{\mathcal{T}}^f$, $c_2^f = K_{\mathcal{T}_2} N_{\mathcal{T}}^f \oplus ID$ and $c_3^f = h(c_1^f, K_{\mathcal{T}_2} N_{\mathcal{R}}^f)$. Finally, $\mathcal{T}$' sends c_1^f, c_2^f, and c_3^f to $\mathcal{A}$ (who, again, is acting as a reader).
3. $\mathcal{A}$ stores c_1^f and c_2^f in the f-th row of Tab.

Phase 3 (Decision): To decide whether $\mathcal{T}$' is the target tag $\mathcal{T}$, the adversary checks:

- $\mathcal{T} \neq \mathcal{T}'$ if $\exists\ (c_1^j, c_2^j) \in Tab$ and $(c_1^f, c_2^f) \in Tab'$ such that $(c_1^j)_m = (c_1^f)_n$ but $(c_2^j)_m \neq (c_2^f)_n$, for all $0 \leq j \leq N$, $0 \leq f \leq N'$ and $0 \leq m, n \leq r-1$.
- Otherwise $\mathcal{T}$= $\mathcal{T}$'.

The total complexity of the given attack is N sessions in the learning phase plus N' sessions in the execution phase. The adversary's advantage, $Adv_{\mathcal{A}}$, to make the correct decision in the third phase of the attack is defined as:

$$Adv_{\mathcal{A}} = \left| Pr[\mathcal{A}^{\mathcal{T}=\mathcal{T}'} \Rightarrow 1] - Pr[\mathcal{A}^{\mathcal{T}\neq\mathcal{T}'} \Rightarrow 1] \right| \tag{3.1}$$

In order to determine $Adv_{\mathcal{A}}$, we have to take into account the following considerations:

1. There are N entries in Tab, each of which includes a value for c_1 with r columns. There are, therefore, $N \times r$ columns in total. Similarly, there are $N' \times r$ columns for the values of c_1 in Tab'.
2. For each $(c_1^j)_m \in Tab$ and $(c_1^f)_n \in Tab'$ we have $(c_1^j)_m = (c_1^f)_n$ with probability 2^{-d}. Consequently, the expected number of matching columns for c_1 in Tab with those in Tab' is $(N \times r) \times (N' \times r) \times 2^{-d}$.
3. Given that $(c_1^j)_m = K_{\mathcal{T}_1}(N_{\mathcal{T}}^j)_m$ and $K_{\mathcal{T}_1}$ is a nonsingular, if $(c_1^j)_m = (c_1^f)_n$ and $\mathcal{T}$=$\mathcal{T}$', then with probability 1 we have $(N_{\mathcal{T}}^j)_m = (N_{\mathcal{T}}^f)_n$ and $(c_2^j)_m = (c_2^f)_n$. However, if $(c_1^j)_m = (c_1^f)_n$ and $\mathcal{T} \neq \mathcal{T}'$, then with probability 2^{-d} we have $(c_2^j)_m = (c_2^f)_n$. Therefore, the probability of incorrectly believing that $\mathcal{T}$= $\mathcal{T}$' when in fact $\mathcal{T} \neq \mathcal{T}'$ is given by:

$$Pr[\mathcal{A}^{\mathcal{T}\neq\mathcal{T}'} \Rightarrow 1] = \left(2^{-d}\right)^{(N\times r)\times(N'\times r)\times 2^{-d}} \tag{3.2}$$

In summary, the adversary's advantage to successfully trace the target tag is:

$$\begin{aligned} Adv_{\mathcal{A}} &= |Pr[\mathcal{A}^{\mathcal{T}=\mathcal{T}'} \Rightarrow 1] - Pr[\mathcal{A}^{\mathcal{T}\neq\mathcal{T}'} \Rightarrow 1] \\ &= 1 - (2^{-d})^{(N\times r)\times(N'\times r)\times 2^{-d}} \end{aligned} \tag{3.3}$$

The probability of success given by (3.3) is considerably high for a sufficient number of eavesdropped sessions (N and N'), allowing an attacker to successfully trace a tag with probability $>> 1/2$. (Note that the value $1/2$ would be the advantage in the ideal case when location privacy location is guaranteed.) Assume, for instance, that 256-bit keys are chosen (*e.g.*, by using 16×16 matrices, *i.e.*, $d = 16$), and that random numbers have size 128 bits through 16×8 matrices and, therefore, $r = 8$. In this case, if the attacker is able to eavesdropped just $N = 32$ sessions during the learning phase of the attack, and another $N' = 32$ sessions during the execution phase, he will succeed with a probability $Adv_{\mathcal{A}} \geq 1 - 2^{-16}$, which is almost equal to 1. Figure 3.2 shows the probability of success of the attack for the most common values of $l = d^2$ in current RFID tags.

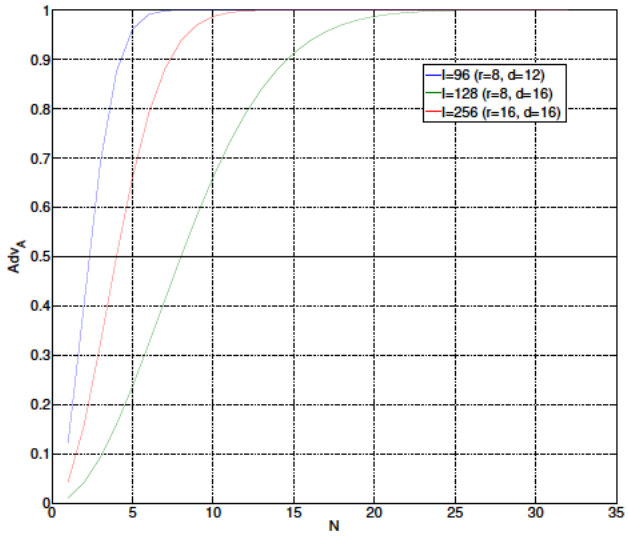


Figure 3.2: Probability of success of the location attack as a function of the number of eavesdropped sessions.

Finally, an interesting point of the proposed attack is that the adversary could even be run passively. In this case, instead of sending the queries to tags $\mathcal{T}$ and $\mathcal{T}$', the adversary would wait for interaction with these tags and then eavesdrops their communications with the legitimate reader $\mathcal{R}$.

3.4 ISO Standard

ISO-IEC 9798 is a set of protocol families which were created by two different committee ISO and IEC for entity authentication and this standard has been widely used on RFID systems. It is consisted of 6 parts:

1. ISO/IEC 9798-1 presents an authentication model as well as general guidelines for entity authentication.
2. ISO/IEC 9798-2 defines 6 protocols based on symmetric-key cryptography.
3. ISO/IEC 9798-3 defines 7 protocols based on cryptographic signatures, of which five were present in the original standard ISO/IEC 9798-3:1998, and the two remaining were introduced in the amendment Amd 1:2010.
4. ISO/IEC 9798-4 defines 4 protocols based on cryptographic check or hash functions.
5. ISO/IEC 9798-5 defines protocols based on zero knowledge techniques.
6. ISO/IEC 9798-6 deals with manual techniques for data transfer between authenticated devices.

In the following subsections parts 1 to 5 are scrutinized in order to clarify how this standard can be applied to different RFID systems.

Most of the protocols defined in the standard use three different types of random numbers called nonces which may vary depending of the requirements: random numbers, sequence numbers, and timestamps. Those are used no more than once for the same purpose and this is usually done to prevent undetectable replay. To

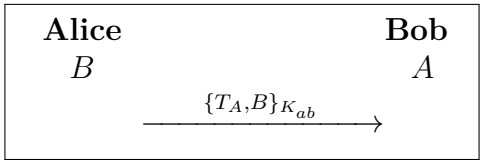


Figure 3.3: ISO/IEC 9798-2: Unilateral Authentication with Timestamps

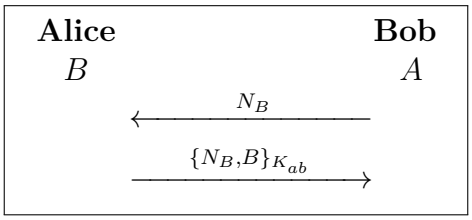


Figure 3.4: ISO/IEC 9798-2: Unilateral Authentication with Nonces

know more about these three types of random numbers we encourage reader to consult details in [116].

3.4.0.1 ISO/IEC 9798 Part 1

ISO/IEC 9798-1 mainly describes the general model for the entity authentication mechanisms of all parts of the standard. This part presents definitions and notations, describes the authentication model and gives some requirements and constraints which are shared with other parts of the standard. Additionally it has some information about how should be used text fields, time variant parameters such as time stamps, sequence numbers, or random numbers, and finally the use of certificates.

3.4.0.2 ISO/IEC 9798 Part 2

ISO/IEC 9798-2 describes 6 different protocol with the required content of messages for entity authentication. Four of these protocols are intended to provide entity authentication without key establishment *i.e.*, without a Trusted Third Party (TTP) and can be split on whether timestamps (T_x) and a nonce (N_x) is used to freshness. Additionally, entity authentication can be either unilateral which means that only one entity is authenticated or bilateral (mutual authentication) which means that both entities are authenticated by increasing the messages exchanged.

1. *Unilateral Authentication with Timestamps* - Alice and Bog share a symmetric key in advance. Alice is authenticated by Bob because Alice introduces the identifier B ensuring that Alice has knowledge of Bob. This protocol can be seen in Fig. 3.3.
2. *Unilateral Authentication with Nonces* - The claimant Alice initiates the communication sending a single message to the verifier Bob who authenticates Alice. This protocol has the same properties as the one with timestamps. Once Bob has received the message, $\{N_B, B\}_{K_{ab}}$ is decrypted and thus the correctness of the identifier B and the nonce N_B are checked. This protocol can be seen in Fig. 3.4.

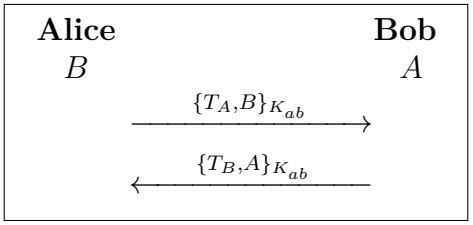


Figure 3.5: ISO/IEC 9798-2: Mutual Authentication with Timestamps

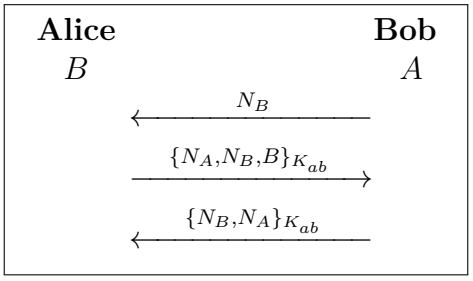


Figure 3.6: ISO/IEC 9798-2: Mutual Authentication with Nonces

3. *Mutual Authentication with Timestamps* - This protocol is built from two instances of the first one providing mutual authentication between Bob and Alice. This protocol can be seen in Fig. 3.5.
4. *Mutual Authentication with Nonces* - This forth protocol is a consequence of the second protocol with some modifications to allow mutual authentication. Thus this is achieved by increasing the length of the message (both nonces are bound) and by introducing an additional message in order to Bob can be authenticated by Alice. This protocol can be seen in Fig. 3.6.
5. The last two protocols where a TTP takes place, are basically the same as in the ISO/IEC 11770-2 standard. In these protocols, entities share symmetric keys with the TTP instead of sharing symmetric keys among themselves. The symmetric session key K_{ab} shared between Alice and Bob is generated by TTP and is sent to both Alice and Bob in a digital envelope. After receiving that message from the TTP, Alice sends a message with this new data to Bob to be authenticated. In mutual authentication, Bob additionally sends back to Alice a message after being authenticated and thus Bob can be authenticated by Alice.
6. *Unilateral Authentication with Nonces and TTP* - In this protocol, Alice sends an encrypted message to the TTP which checks its authenticity and finally the TTP replies by: 1) sending back a nonce to Alice to check that the key was received and 2) sending a timestamp to Bob to check freshness. Finally the session key K_{ab} is chosen by Alice. This protocol can be seen in Fig. 3.7.
7. *Mutual Authentication with Nonces and TTP* - In this final protocol, and optional handshake is also introduced by Alice. The main difference with the protocol described above is that in this case, Bob is who chooses the session key K_{ab} and thus both entities are mutually authenticated. This protocol can be seen in Fig. 3.8.

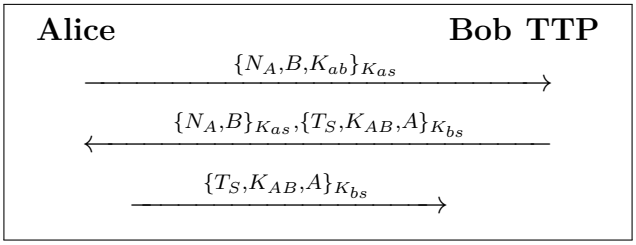


Figure 3.7: ISO/IEC 9798-2: Unilateral Authentication with Nonces and TTP

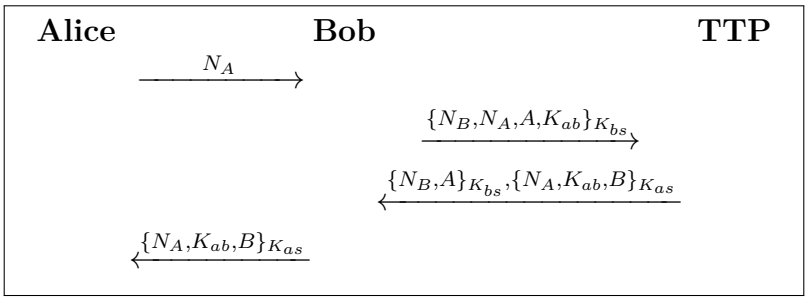


Figure 3.8: ISO/IEC 9798-2: Mutual Authentication with Nonces and TTP

3.4.0.3 ISO/IEC 9798 Part 3

Five protocols are described in the ISO/IEC 9798-3 where two of them are for unilateral authentication and the other three mechanisms are for mutual authentication. Messages are exchanged between the claimant and the verifier for the verification of the claimant's identity in the unilateral authentication or both entities are verified in the mutual authentication. The standard has some flexibility for some text fields which may be included or not in the protocol for some security reasons such as information authentication, add extra redundancy to the signature or to provide validation among others. Timestamps, counters or random numbers can be added to provide freshness of the messages.

1. *Unilateral Authentication with Timestamps* - Alice and Bog share a symmetric key in advance. This protocol guarantees to Bob that Alice is alive (T_A), as well as providing assurance that Alice is aware of Bob as her peer entity ($Sig_A(T_A, B)$). This protocol can be seen in Fig. 3.9.
2. *Unilateral Authentication with Nonces* - Alice and Bog share a symmetric key in advance. This protocol is essentially the same as the one described above. However it has two main differences: 1) timestamps are substituted by nonces; 2) the nonce N_A chosen by Alice to ensure that Alice is not signing messages already chosen by Bob, but this may generate some problems to Alice if the signature and the key are also used again in other applications. This protocol can be seen in Fig. 3.10.
3. *Mutual Authentication with Timestamps* - This protocol is a combination of two instances of the first one providing thus mutual authentication for both entities. Note that messages are not dependent and this protocol may be executed only in one round. This protocol can be seen in Fig. 3.11.
4. *Mutual Authentication with Nonces* - This forth protocol is an extension of the

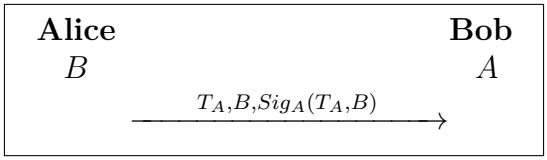


Figure 3.9: ISO/IEC 9798-3: Unilateral Authentication with Timestamps

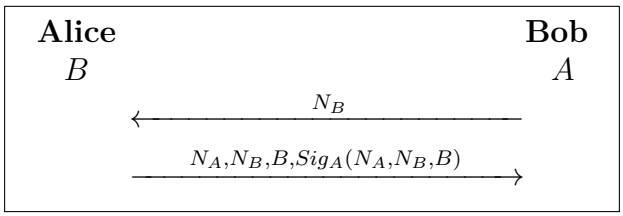


Figure 3.10: ISO/IEC 9798-3: Unilateral Authentication with Nonces

second one where timestamps are used. Additionally, mutual authentication is allowed by sending back a message from Bob to Alice. Note that messages in this protocol are dependent and cannot be answered in advance. This protocol can be seen in Fig. 3.11.

5. *Parallel Mutual Authentication with Nonces* - This last protocol is an improvement of the fifth one allowing authentication in parallel between Alice and Bob. This could be done due to the exchange of N_A and N_B as the first part of the protocol. Note that this operation can be done in parallel and thus the last two messages can be run in parallel too. This protocol can be seen in Fig. 3.13.

3.4.0.4 ISO/IEC 9798 Part 4

This part of ISO/IEC 9798-4 specifies four entity authentication protocols using a cryptographic check function. This is particularly interesting when there is no need to recover the components of the function due to the computational costs. Additionally, the standard does not specify if messages can or not contain text fields and the relationship they have. Note that this part, according to the standard, could be used for key distribution protocols.

The structure is similar to others parts of the standard: first two mechanisms are concerned with unilateral authentication, while the other two are mechanisms for mutual authentication. The algorithms proposed can be seen in Fig. 3.14 where unilateral authentication is used and in Fig. 3.15 where mutual authentication is implemented. Note that, ISO/IEC 9798-2 is equal to this protocol however a hash function is used instead of symmetric encryption.

According to this part of the standard, if a time stamp or sequence number is used, one pass is needed for unilateral authentication and another one more to achieve mutual authentication. On the other hand, if random numbers are used instead of timestamps, two passes are needed for unilateral authentication and one more to achieve mutual authentication.

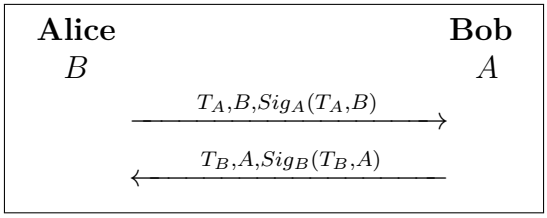


Figure 3.11: ISO/IEC 9798-3: Mutual Authentication with Timestamps

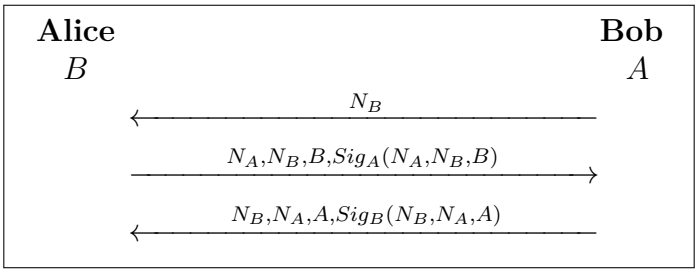


Figure 3.12: ISO/IEC 9798-3: Mutual Authentication with Nonces

3.4.0.5 ISO/IEC 9798 Part 5

ISO/IEC 9798-5 specifies entity authentication mechanisms using zero-knowledge techniques. These mechanisms rely on the use of random numbers not only as challenges, but also as commitments to prevent bad behaviours and cheating. This can be achieved by allowing a prover to demonstrate knowledge of a secret while no more information is published. This part can be grouped into five sets according to the nature of the zero-knowledge techniques. All of them provide unilateral authentication but only those who are based on asymmetric encryption and elliptic curves allow both unilateral and mutual authentication:

- Identities.
- Integer factorization.
- Discrete logarithms with respect to numbers that are either prime or composite.
- Asymmetric encryption.
- Discrete logarithms on elliptic curves (note that these mechanisms are constructed according to the zero-knowledge basis, however they are not necessarily zero-knowledge because of the parameter's choice).

Moreover, according to the type of calculation this part can be classified into four main groups [79]:

1. Short modular exponentiations. The challenge size needs to be optimized since it has a proportional impact on workloads.
2. Possibility of a "coupon" strategy for the claimant. A verifier can authenticate a claimant without computational power. The challenge size has no impact on workloads.
3. Possibility of a "coupon" strategy for the verifier. A verifier without computational power can authenticate a claimant. The challenge size has no impact on workloads.
4. No possibility of a "coupon" strategy.

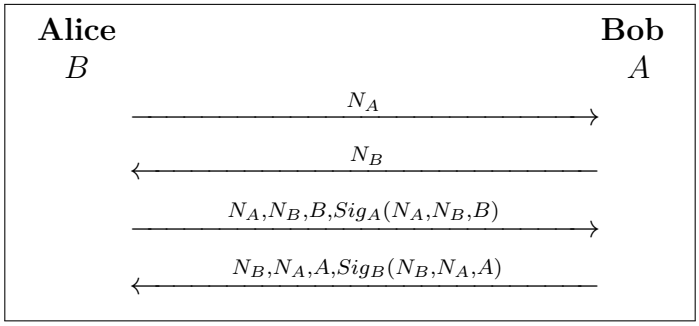


Figure 3.13: ISO/IEC 9798-3: Parallel Mutual Authentication with Nonces

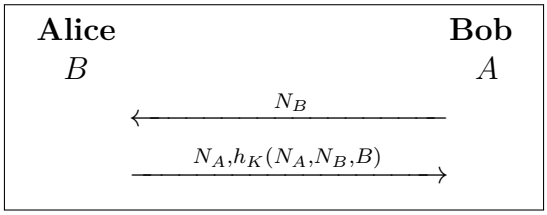


Figure 3.14: ISO/IEC 9798-4: Unilateral Authentication with Nonces

Well known examples of zero-knowledge protocols which are commonly use as an extension of this standard are Fiat-Shamir [59], Gillou-Quisquarter [68] and Schnorr's [148] identification protocols. Comparison and attacks can be read in Chapter 10 of [116].

3.4.0.6 ISO/IEC 9798 Part 6

This last part of the standard, ISO/IEC 9798-6, specifies four entity authentication mechanisms based on manual data transfer between authenticating devices. In this part, the term entity authentication is completely different from the rest parts of the standards. Here, both parties check that they share the same data string at the same execution time of the mechanism instead of verifying the identity each party. This could be particularly appropriate in some kind of personal area networks or networks where there is no need for an existing public key infrastructure, shared secret keys or passwords where, for example two personal devices need to authenticate themselves to perform some actions. It is worth saying that these mechanisms may also be used to support key management functions.

As an example of data authentication, MANA certificate is presented in section 6.2.3 of the standard [80]. MANA has two components: a key (K) which is generated in a random way and a check value (CV) which is computed from the key and the data ($Data$). The protocol can be seen in Fig. 3.16.

For more information all original parts of the standard are in [79, 80, 81, 82, 83]. A recent publication where part 2 is analysed under an automatic tool for analysing security protocols named AVISPA can be seen in [182]. A depth analysis of ISO/IEC 9798 is done in a technical report in [18] while some improvements over the standard can be read in [19, 20] and additional references can be read in [12, 32, 116]

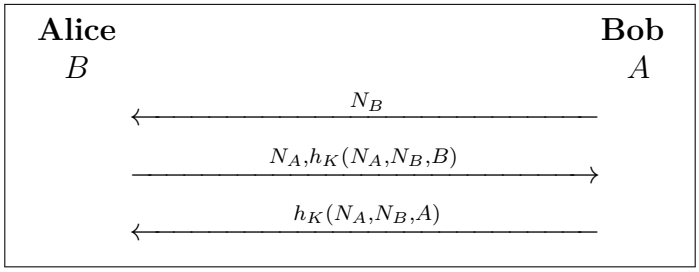


Figure 3.15: ISO/IEC 9798-4: Mutual Authentication with Nonces

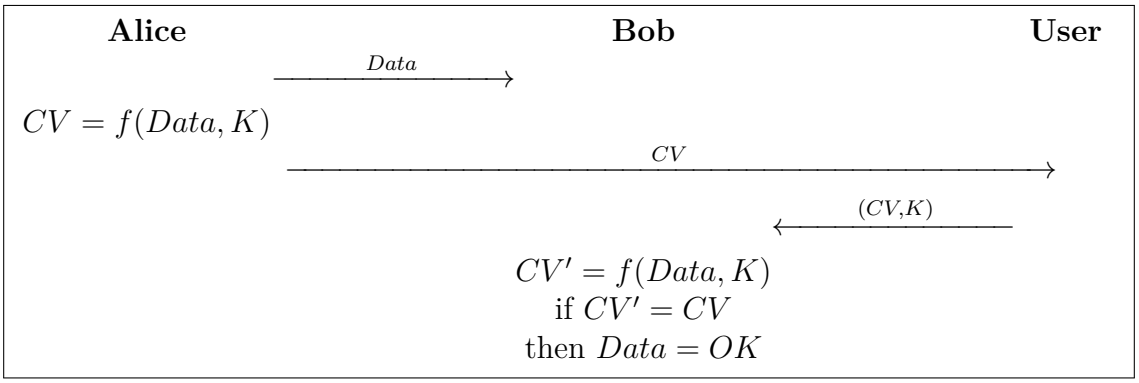


Figure 3.16: ISO/IEC 9798-6: MANA certificate

3.5 Standard-based RFID Health Protocols

Nowadays there are a significant number of proposals on RFID authentication protocols (see, *e.g.*, [50, 61, 138]), some of which have a clear focus on health applications, such as for example [109, 144, 174]). Nevertheless, the vast of majority of these schemes, like the one in [164] analyzed in this section, suffer from various flaws and have been proven to be insecure [40, 46, 76, 133]. This is mainly caused by the usage of non-standard approaches that ignore prudent practices and well-established principles in the design of security protocols, as well as a lack of rigorous security analysis. In particular, Wu *et al.*'s scheme offers a rather standard gaming-based security analysis, but the authors miscalculate probabilities. One major weakness of this proposal lies in using a matrix multiplication-based classical cipher (Hill) as cryptographic primitive for encryption. This is an old and largely insecure mechanism [45, 64] that open doors to attacks like the one presented in this section.

Even though current passive RFID tags have rather limited on-chip capabilities, they support some cryptographic functions, especially lightweight ones that have been recently developed for this type of applications. Later in subsection 3.5.3 we discuss implementation aspects and suggest specific algorithms to carry out these functions. Building upon this assumption, in this subsection we introduce two RFID security mechanisms based on existing standard designs adapted to healthcare environments. As a motivating examples, we will use two practical scenarios sketched in Figures 3.17 and 3.18. The first case illustrates a typical application where mutual authentication between two medical entities (*e.g.*, a doctor and a patient, or a doctor and a blood container) is required. The second scenario motivates the

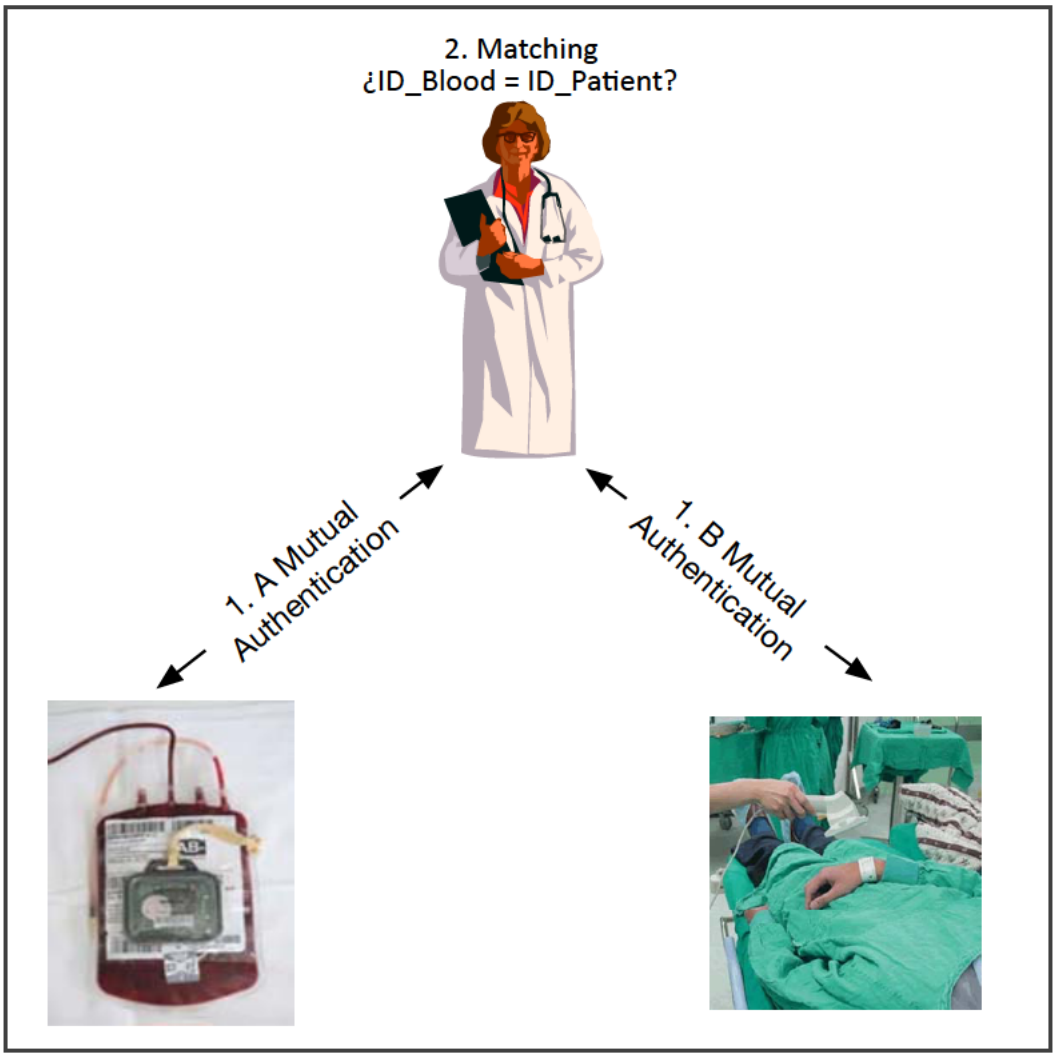


Figure 3.17: Blood-handling scenario.

need for secure channels to access to an IMD a pacemaker, in this case , which requires mutual authentication, key establishment and secure messaging. Note that the security core running on-chip of the implant is functional and computational equivalent to the one supported on a RFID tag.

The notation used throughout this section is summarized in Table 3.3.

3.5.1 Entity Authentication

There is a wide variety of applications in a hospital where secure and efficient authentication mechanisms are demanded. For instance, RFID technology may be used to prune blood-handling errors. This process consists of two phases. First the identities of the patients and blood bags are confirmed (authentication protocol) and then the matching between both entities is checked (verification step). The process is sketched in Fig. 3.17 and an authentication protocol is at the core of this application.

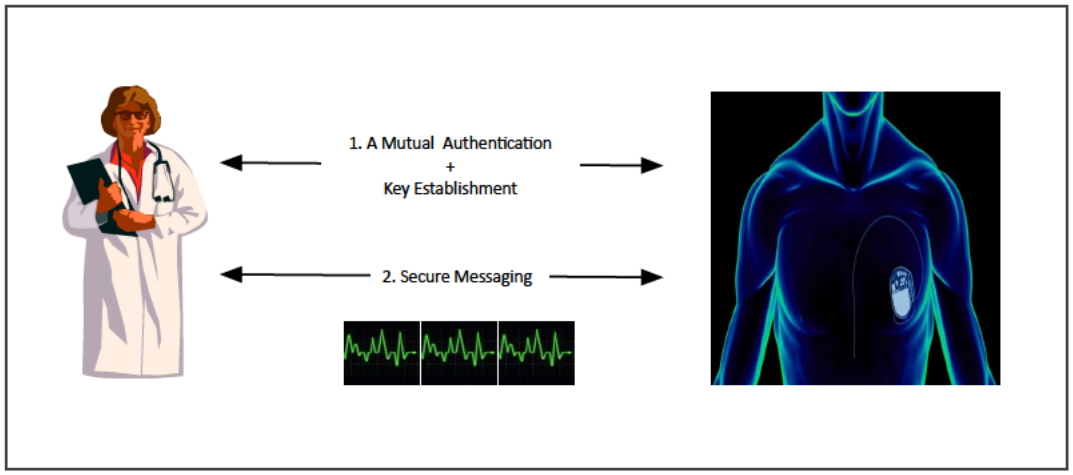


Figure 3.18: Secure messaging scenario.

ISO/IEC 9798 Part 2 [82] specifies six schemes based on symmetric encryption algorithms. Four of these protocols provide entity authentication alone, while the last two ones provide also key establishment. Our proposed scheme is based on the fourth protocol of this standard and guarantees mutual authentication. Furthermore, the peculiarities of RFID systems like the anonymous identification through the insecure radio channel have been taken into account in our design.

The entities involved are three: the tag ($\mathcal{T}$), the reader ($\mathcal{R}$) and the database ($\mathcal{DB}$). $\mathcal{T}$ and $\mathcal{DB}$ share an authentication key (K_{ENC_TB}), a message authentication key (K_{MAC_TB}), and their identifiers are $ID_{\mathcal{T}}$ and $ID_{\mathcal{DB}}$, respectively. Tags are anonymously identified by the use of pseudonyms ($IDS_{\mathcal{T}}$), which are updated once the authentication process has been successfully completed. On the other hand, a copy of the old and current values ($IDS_{\mathcal{T}}^{new}$, $IDS_{\mathcal{T}}^{old}$) are held in the database to avoid de-synchronization attacks. The database keeps a table in which each row stores the information of a particular tag: $\{IDS_{\mathcal{T}}^{\{new,old\}}, K_{ENC\_TB}, K_{MAC\_TB}\}$. The pseudonym is used as a search index in the database to retrieve the information linked to the interrogated tag (K_{ENC_TB}, K_{MAC_TB}). The protocol makes use of four cryptographic primitives: an encryption algorithm, a MAC algorithm, a one-way compression function and a pseudo-random number generator. The exchanged messages, shown in Figure 3.19, in our three-pass mutual authentication protocol are described bellow:

Step 1: $\mathcal{R} \rightarrow \mathcal{T}$: $N_{\mathcal{R}}$. The reader sends a query signal and a random value $N_{\mathcal{R}}$ to the tag.

Step 2: $\mathcal{T} \rightarrow \mathcal{R}$: $\mathrm{N}_{\mathcal{T}}, c_0, c_1, c_2$. The tag generates a random number $\mathrm{N}_{\mathcal{T}}$ and computes a fresh version of its pseudonym ($c_0 = h(IDS_{\mathcal{T}}, \mathrm{N}_{\mathcal{T}}, \mathrm{N}_{\mathcal{R}})$) that facilitates its anonymous identification. Then $\mathcal{T}$ computes an encrypted message that includes both the random number received and the one generated on-board, and its static identifier ($c_1 = [[\mathrm{N}_{\mathcal{T}}, \mathrm{N}_{\mathcal{R}}, ID_{\mathcal{T}}]]_{K_{ENC\_TB}}$). Finally a MAC is computed ($c_2 = \{c_1\}_{K_{MAC\_TB}}$) and all these aforementioned values (*i.e.*, $\{c_0, c_1, c_2\}$) together with the nonce $\mathrm{N}_{\mathcal{T}}$ are sent to the reader and finally forwarded to the database.

$\mathcal{T}$ and $\mathcal{I}$:	Tag and IMD
$\mathcal{DB}$:	Back-end Server (database)
ID_X:	Identification number of entity X
SSC:	Send Sequence Counter
F_{XY} :	Keying material sent from X to Y
ACK	Acknowledge message
ERR:	Error message
K_{ENC_XY}:	Authentication key shared between entities X and Y
K_{MAC_XY}:	Message authentication key shared between entities X and Y
KS_{ENC_XY}:	Authentication session key shared between entities X and Y
KS_{MAC_XY}:	Message authentication session key shared between entities X and Y
$[[M]]_K$	Encryption of message M with key K to provide confidentiality
$\{M\}_K$	Message Authentication Code (MAC) of message M with key K to provide integrity
$h(\cdot)$	One-way compression function
$f(\cdot)$	Key Derivation Function (KDF)

Table 3.3: Notation used in the proposed authentication and secure messaging schemes for health applications.

Step 3: $\mathcal{DB} \rightarrow \mathcal{T}$: $\{c_3, c_4\}$. The back-end searches in its table the entry that satisfies the value c_0. More precisely, at the n-row it retrieves the new and old index-pseudonyms and computes a local version of c_0 (*i.e.*, c_0^{new} and c_0^{old}). Then $\mathcal{DB}$ checks whether one of the above values fits with the received one. If yes, the tag is identified and its associated values are retrieved $\{K_{ENC\_TB}, K_{MAC\_TB}\}$. Otherwise, the above process is executed with the next entry (n+1-row) in the table. The process is repeated until a match is found or the end of the table is reached. The protocol is interrupted at this step if no matching occurred and all the entries were checked. If not, once the tag is identified, the database computes a local version of the MAC ($(c_2' = \{c_1'\}_{K_{MAC\_TB}})$) and checks its equality with the received value. The protocol is aborted whether the above checking fails. Otherwise, $\mathcal{DB}$ decrypts c_1 and obtains the identifier of the target tag ($ID_{\mathcal{T}}$). At this step the tag is authenticated (one-side authentication). Then, the database encrypts the random numbers linked to the session ($c_3 = [[\mathrm{N}_{\mathcal{R}}, \mathrm{N}_{\mathcal{T}}]]_{K_{ENC\_TB}}$), computes a MAC ($c_4 = \{c_3\}_{K_{MAC\_TB}}$), and both values are sent to the tag. Finally the current pseudonym is held and the new pseudonym is updated using the one-way compression function: $IDS_{\mathcal{T}}^{old} = IDS_{\mathcal{T}}^{new}$ and $IDS_{\mathcal{T}}^{new} = h(IDS_{\mathcal{T}}^{new})$.

Step 4: $\mathcal{T}$: The tag calculates a local version of the MAC ($c_4' = \{c_3'\}_{K_{MAC\_TB}}$) and decrypts message c_3. If the MAC is correct and the nonces obtained match with the nonces associated with the current session, the server is authenticated. Therefore both sides are authenticated at this point and the mutual authentication process finishes successfully. Finally, the tag updates its pseudonym ($IDS_{\mathcal{T}} = h(IDS_{\mathcal{T}})$). On the contrary, if some of the above checkings were wrong, the tag sends an error message and an alarm is triggered in the protocol the pseudonym updating is not executed in this case.

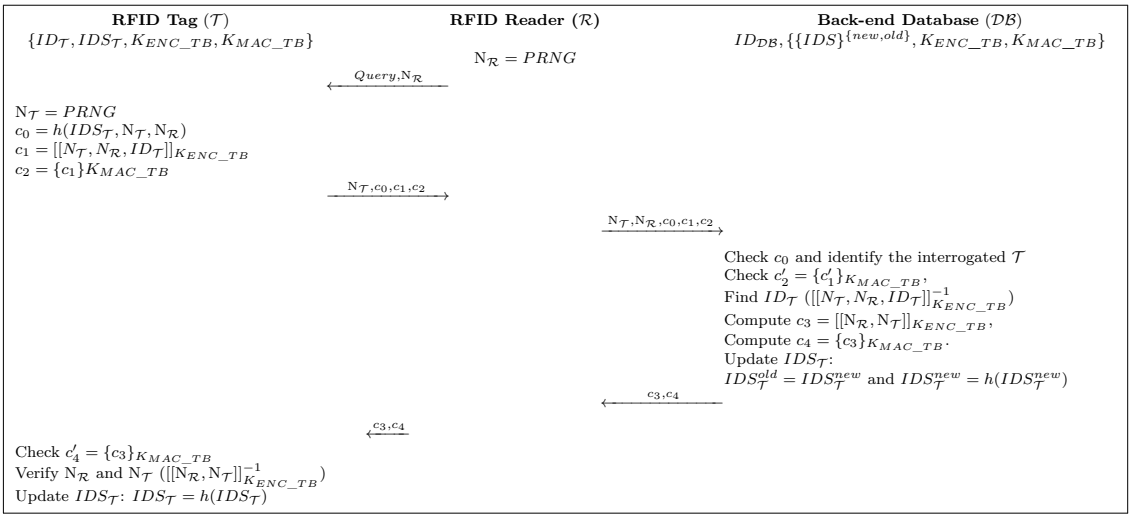


Figure 3.19: Entity Authentication Protocol

3.5.2 Secure Messaging

Apart from authentication, there are many medical applications that demand the exchange of private information. For instance, nowadays the new generation of medical implants possess wireless connectivity. Imagine a doctor equipped with a reader aims to access the records of vital signals stored on the memory of an implant. In this scenario, the doctor (reader) and the patient (implant) are first mutually authenticated and then a secure exchange of data can be performed. The process is displayed in Figure 3.18 and the details are given below.

Thirteen protocols using symmetric encryption algorithms are specified in the ISO/IEC 11770 Part 2 standard. Six of them are server-less, while the other seven require a trusted server. As in electronic passports [77], we opt for ISO-IEC 11770 Mechanism 6. Moreover, the special characteristics of wireless-medical systems like the anonymous identification through an insecure (radio) channel or its energy restrictions have been considered.

The entities involved in the protocol are the implant ($\mathcal{I}$), the reader ($\mathcal{R}$) and the database ($\mathcal{DB}$). $\mathcal{I}$ and $\mathcal{DB}$ share an authentication key (K_{ENC_IB}), a message authentication key (K_{MAC_IB}), and its identifiers are $ID_{\mathcal{I}}$ and $ID_{\mathcal{DB}}$, respectively. The anonymous identification of implants is guaranteed by the use of pseudonyms ($IDS_{\mathcal{I}}$), which are updated once the authentication process has been successfully completed. At the same time, a copy of the old and current values ($IDS^{new}_{\mathcal{I}}$, $IDS^{old}_{\mathcal{I}}$) are held in the database to avoid de-synchronization attacks. The database keeps a table in which each row stores the information of a particular implant: $\{IDS^{\{new,old\}}_{\mathcal{I}}, K_{ENC\_IB}, K_{MAC\_IB}\}$. The pseudonym is used as a search index in the database to retrieve the information linked to the interrogated implant (K_{ENC_IB}, K_{MAC_IB}). The scheme requires an encryption algorithm, a MAC algorithm, a one-way compression function, a pseudo-random number generator, and a KDF. The exchanged messages, shown in Figure 3.20, in our three-pass mutual authentication protocol plus two-pass secure messaging scheme are described bellow:
Step 1: $\mathcal{R} \rightarrow \mathcal{I}$: $N_{\mathcal{R}}$. The reader sends a query signal and a random value $N_{\mathcal{R}}$ to

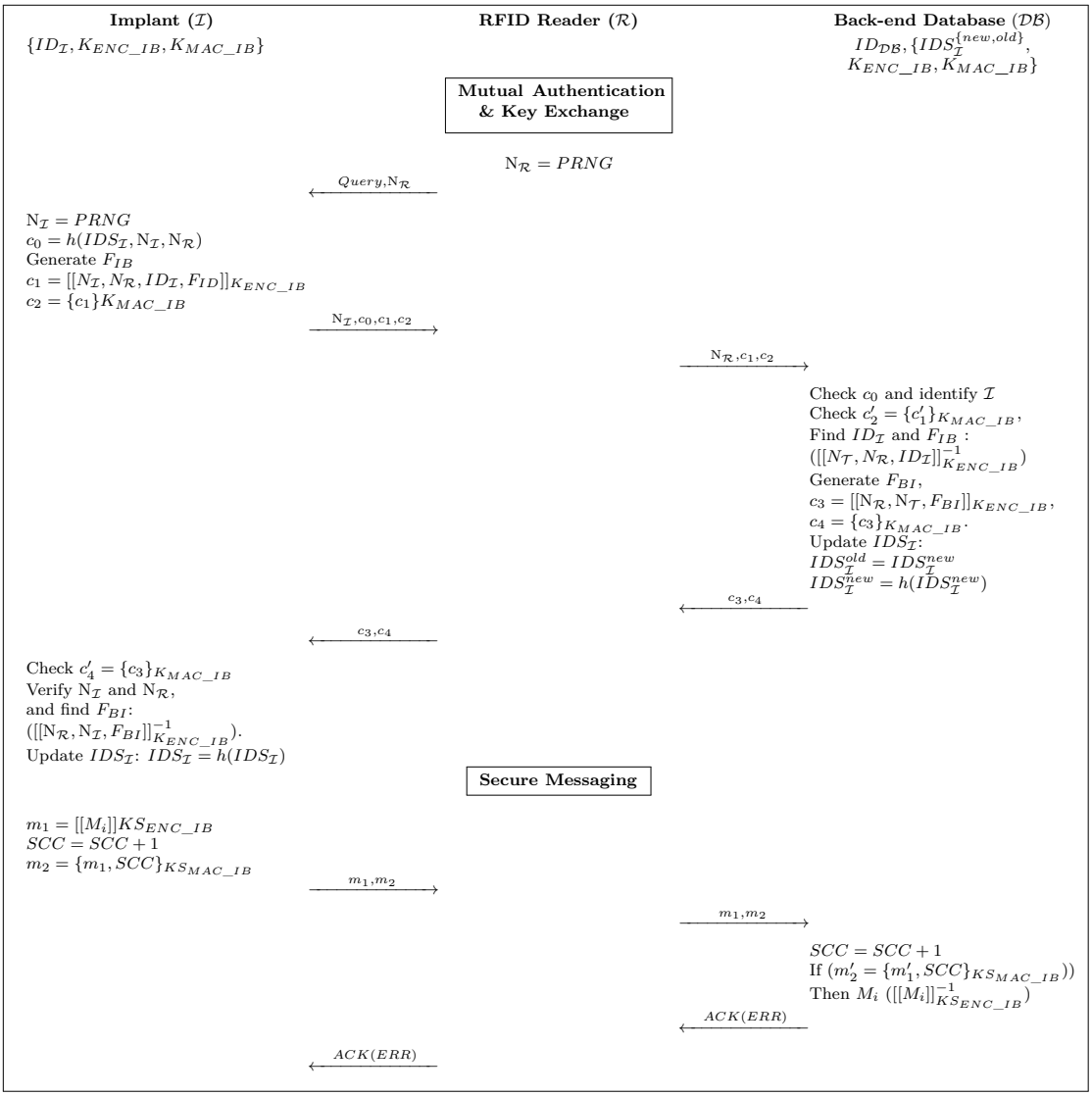


Figure 3.20: Secure Messaging Scheme

the implant.

Step 2: $\mathcal{I} \rightarrow \mathcal{R}$: $N_{\mathcal{I}}, c_0, c_1, c_2$. The implant generates a random number ($N_{\mathcal{I}}$) and keying material (F_{IB}) and computes a fresh version of its pseudonym ($c_0 = h(IDS_{\mathcal{I}}, N_{\mathcal{I}}, N_{\mathcal{R}})$) that facilitates its anonymous identification. Then $\mathcal{I}$ computes an encrypted message that includes the random number received and the one generated on-board, keying material, and its static identifier ($c_1 = [[N_{\mathcal{I}}, N_{\mathcal{R}}, ID_{\mathcal{I}}, F_{IB}]]_{K_{ENC\_IB}}$). Then a MAC is computed ($c_2 = \{c_1\}_{K_{MAC\_IB}}$) and the aforementioned values (*i.e.*, $\{c_0, c_1, c_2\}$) together with the nonce $N_{\mathcal{I}}$ are sent to the reader and finally forwarded to the database.

Step 3: $\mathcal{DB} \rightarrow \mathcal{T}$: $\{c_3, c_4\}$. The back-end searches in its table the entry that satisfies the value c_0. In detail, at the n-row it retrieves the new and old index-pseudonyms and computes a local version of c_0 (*i.e.*, c_0^{new} and c_0^{old}). Then $\mathcal{DB}$ checks whether one of these computed values fits with the received one. If yes, the implant is identified and its associated values are retrieved

$\{K_{ENC\_IB}, K_{MAC\_IB}\}$. Otherwise, the above process is executed with the next entry (n+1-row) in the table. The process is repeated until a match is found or the end of the table is reached. The protocol is interrupted at this step if no matching occurred and all the entries were checked. If not, once the implant is identified, the database computes a local version of the MAC ($c_2' = \{c_1'\}_{K_{MAC\_IB}}$) and checks its equality with the received value. If the above checking fails, the protocol is aborted. Otherwise, $\mathcal{DB}$ decrypts c_1 and obtains the identifier of the implant ($ID_{\mathcal{I}}$) and the keying material generated by the other side (F_{IB}). At this step, the implant is authenticated (one-side authentication). Next, the database generates keying material (F_{BI}) and encrypts this value together with the nonces linked to the session ($c_3 = [[\mathrm{N}_{\mathcal{R}}, \mathrm{N}_{\mathcal{I}}, F_{BI}]]_{K_{ENC\_IB}}$) and computes a MAC ($c4 = \{c_3\}_{K_{MAC\_IB}}$). After that, both values are sent to the implant. Finally the current pseudonym is held and the new pseudonym is updated using the one-way compression function: $IDS_{\mathcal{I}}^{old} = IDS_{\mathcal{I}}^{new}$ and $IDS_{\mathcal{I}}^{new} = h(IDS_{\mathcal{I}}^{new})$.

Step 4: $\mathcal{I}$: The implant calculates a local version of the MAC ($c4' = \{c_3'\}_{K_{MAC\_IB}}$) and decrypts message c_3. If the MAC is correct and the nonces obtained match the nonces associated with the current session, the server is authenticated. Thus, both sides are authenticated at this step, the mutual authentication process finishes successfully and the implant updates its pseudonym ($IDS_{\mathcal{I}} = h(IDS_{\mathcal{I}})$). If some of the above checkings were wrong, the implant sends an error message, an alarm is triggered in the protocol, and the pseudonym updating is not executed. Note that, apart from authentication, the implant also received the keying material from the database (F_{BI}).

Step 5: Session Key Derivation: Once authentication is completed, the implant and the database calculate the session keys. We use a Key Derivation Function (KDF; $f(\cdot)$) with two inputs (F_{IB} and F_{BI}). In particular, we follow the KDF in counter mode specified in NIST 800-108 recommendation (see Sect. 5.1 in [123] for details). Following this algorithm, two fresh keys KS_{ENC_IB} and KS_{MAC_IB} are shared between both entities. Furthermore, as in [77] specification (see page IV-40; Section A.5.4.2) a Send Sequence Counter (SSC) is computed from the two random numbers linked to the session: *e.g.*, $SSC = \mathrm{N}_{\mathcal{I}}$ (2 least significant bytes), N_B (2 least significant bytes).

After that, a secure exchange of data can be accomplished. For each data block (M_i) the following procedure is followed:

Step 6: $\mathcal{I} \rightarrow \mathcal{DB}$: m_1, m_2. First the implant encrypts M_i with KS_{ENC_IB} ($m_1 = [[M_i]]_{KS_{ENC\_IB}}$). Then the MAC of m_1 is computed following three steps: 1) SSC is incremented with 1; 2) SCC is padded to m_1, and 3) the MAC with KS_{ENC_IB} is calculated (*i.e.*, $\{m_1, SCC\}_{KS_{ENC\_IB}}$). Next these two values ($\{m_1, m_2\}$) are sent to the reader and finally forwarded to the database.

Step 7: $\mathcal{I} \rightarrow \mathcal{DB}$: ACK or ERR: The database computes a local version of the MAC. More precisely, SCC is incremented with one and padded to the received m_1' and finally the MAC is computed (*i.e.*, $m_2' = \{m_1', SCC\}_{KS_{ENC\_IB}}$). If both values match, the data block is decrypted ($[[M_i]]^{-1}_{KS_{ENC\_IB}}$) and an acknowledge message (ACK) is sent to the implant. Otherwise, an error message (ERR)

is sent to the implant.

3.5.3 Implementation Aspects

The two applications presented in this section rely on the use of several cryptographic primitives: encryption, one-way compression, MAC, PRNG, and key derivation functions. As we next discuss, the proposed primitives use a block cipher as the core component of each algorithm. RFID tags can be classified regarding its operating frequency or its source of power as described in Section 3.1. On the other hand, price is a crucial factor that determines tag capabilities (*e.g.*, memory and power computation). Low-cost and high-cost tags are the two main classes with respect to this parameter. The size of the chip and, consequently, its capabilities is directly linked to its price. Low-cost tags have a price that varies from 10 to 30 cents, with around 3000-5000 gates equivalents that can be devoted to security purposes [7]. Adequate implementations of standard block ciphers like Advanced Encryption Standard (AES), or modern designs like PRESENT, can be used in such tags [25, 94]. Even though in our proposal all primitives are based on a block cipher, the tag must support several algorithms and it does not seem plausible that all of them would fit in a low-cost tag. Consequently, we recommend the usage of high-cost tags. These have a market price of 1-2 dollars, which is reasonable for medical environments. In this sort of tags, more than 7000 gates equivalents are available for security issues [21, 57], and the overprice is justified by the high security level demanded in medical applications, particularly when the safety of patients is a vital factor in these environments [41, 133].

We next discuss in detail the cryptographic building blocks used in our proposal. As in the case of the protocols presented above, all constructions are based on ISO/IEC standards and NIST recommendations.

3.5.3.1 Encryption Algorithm

The first key aspect is the adoption of symmetric or asymmetric cryptographic approaches. We discard public cryptography due to the current scarcity of resources in constrained devices like low-cost RFID tags or IMDs. Our two proposals described above use a lightweight and secure cipher. We can opt for standard approaches, such as for example the tiny implementation of AES [58] or more recent lightweight block ciphers like PRESENT [28] or KATAN family [36]. Stream ciphers like Grain [73] or Trivium [118] could also be used, but we discard this option since the MAC algorithm will be based on the cipher and stream-cipher-based MAC algorithm are not standardized.

3.5.3.2 One-way Compression Function

A one-way compression function is a function that transforms a fixed-length input into a fixed-length output, being difficult to compute an input given a particular output. This sort of functions are often build using block ciphers like the mentioned in the previous section. In detail, these make use of the following components: 1) a block cipher with block size L, called CIPH and parametrized by a symmetric key

K; 2) a function g with maps L-bit inputs to keys K suitable for CIPH; and 3) a fixed L-bit initial value. In the literature, there are several proposed algorithms: Davies-Meyer, Matyas-Meyer-Oseas and Miyaguchi-Preneel [116]. This latter is described below. The input M (*i.e.*, $h(M)$) is divided into L-bit blocks and padded, if necessary, to completed the last block M_m: $M_1||M_2||\cdots||M_m$, where $m = |M|/L$ and $||$ symbolizes concatenation. Then the algorithm is executed as follows:

Hash Algorithm (Miyaguchi-Preneel construction)
1. $H_0 = IV$
2. For $i = 1$ to m
3. $\quad H_i = CIPH_{g(H_{i-1})}(M_i) \oplus M_i \oplus H_{i-1}$.
4. $T = H_m$
5. Return T

3.5.3.3 MAC Algorithm

We propose the use of a MAC algorithm based on a symmetric-key block cipher, since this primitive is already used in the protocol and we can easily reuse it. This cipher-based MAC is abbreviated as Cipher-based MAC (CMAC). Our algorithm follows the NIST 800-38B Recommendation [122]. We assume that we have a block cipher with block size L, called CIPH, and a shared key (K). Moreover, for sub-key generation we follow the guidelines dictated in [122] (NIST 800-38B, pages 7-8); the sub-keys (K_1 and K_2) are generated and stored in the memory of entities involved (*i.e.*, tag and database) at the key distribution phase. To compute the MAC of message M (*i.e.*, $\{M\}_K$), M is divided into blocks of L bits: $M_1||M_2||\cdots M_m$, where $m = |M|/L$ and $||$ denotes concatenation. As specified in [122], the last block is XORed with $K2$ or $K1$, depending if padding is needed or not.The CMAC algorithm is described below:

CMAC Algorithm (compliant with NIST 800-38B)
1. $C_0 = 0^L$
2. For $i = 1$ to m
3. $\quad C_i = CIPH_K(C_{i-1} \oplus M_i)$.
4. $T = C_m$
5. Return T

3.5.3.4 Pseudo-random Number Generator

Apart from the Hash and MAC algorithms, random numbers are used in the protocol. We opt for an standard approach again. As specified in NIST 800-38A [121] (recommendation for block ciphers modes of operation), we propose the use of a block cipher in counter mode, denoted CTR. The current value of the counter is called T_j and R_N represents the resulting $L/2$-bits random number, L being the block size for the used block-cipher. The initial value of the counter is set at the

key distribution phase, *i.e.*, $T_0 = random\_seed$. After each nonce generation, the counter value is updated to T_{j+1}. The algorithm is described below:

PRNG: Block cipher in CTR Mode (compliant with NIST 800-38A)
1. $O_j = CIPH_k(T_j)$
2. $R_N = \|O_j\|_{0\cdots(L/2-1)}$
3. $T_{j+1} = \|O_j\|_{L/2\cdots L}$

3.5.3.5 Key Derivation Function

As specified in NIST 800-108 [123], we propose the use of a KDF in counter mode and the CMAC primitive is used as the Pseudorandom Function (PRF). The key derivation function is calculated by xoring the keying materials exchanged in the first phase of the protocol ($K_l = F_{ID} \oplus F_{DI}$). Next, the session keys KS_{ENC_IB} and KS_{MAC_IB} are generated. In the following, we assume that the bit length of these keys are r times the length of the used block-cipher with block size L. Depending on whether the key is used for encryption or MAC, the Fixed Input Data (FID) take one of these values: (0x 00 00 00 00 00 01 || 0x 00 || $ID_{\mathcal{I}}$) or (0x 00 00 00 00 00 02 || $0x$ 00 || $ID_{\mathcal{I}}$).

Key Derivation Function – CTR Mode (compliant with NIST 800-108)
1. $result = []$;
2. For $i = 1$ to r, do
3. $\quad K(i) = CMAC_{K_l}(i, FID)$
4. $\quad result(i) = result(i-1) \,\|\| \, K(i)$
5. Return $KS =$ leftmost $(r \cdot L)$ bits of $result$.

3.6 Conclusions

In the last years, several RFID-based solutions have been proposed to solve a variety of problems in healthcare environments. These proposals deal with interesting applications, such as monitoring of Alzheimer patients or intelligent drug administration systems. Unfortunately, the majority of such schemes, like the one by Wu *et al.* [164] analysed in this chapter, have resulted poor from the security point of view [40, 46, 76, 133]. In general, such a lack of security is due to two main reasons: (i) the use of non-standard constructions that do not follow prudent design practices and established recommendations; and (ii) informal and/or non-rigorous security analysis.

With the aim of avoiding these common mistakes, we have proposed two new RFID protocols for healthcare environments based on standards and recommendations. More precisely, the security schemes proposed conform to ISO/IEC 9798 and 11770. The security of the standards included in these specifications has been deeply studied in the literature. This provides, in our opinion, more confidence than ad-hoc

designs. Furthermore, we provide details about implementation aspects by following NIST Security Recommendations. Finally, we hope that schemes such as those here proposed can give support to additional RFID-based healthcare applications and stimulate further research in the area.

4

Secure Publish-Subscribe Protocols for Heterogeneous Medical Wireless Body Area Networks

4.1 Introduction

The development of reasonably powerful wearable sensors and medical devices has stimulated research in WBANs applied to healthcare scenarios. A prototypical scenario is that of a patient equipped with a number of wearable and implantable sensors that constantly measures various health-related parameters. Sensors are networked, meaning that they have communication capabilities and can interact with each other and with a central network controller that provides coordination, long-term storage, etc. The WBAN is often assumed to possess the ability to connect with external entities, for example, through an Internet connection. This would allow healthcare staff to monitor the patient remotely, continuously, and in real time [103], even using automatically generated prognoses of the patient's health conditions with methodologies such as the one proposed in [128]). Overall, the possibilities offered by WBAN technologies in the healthcare domain are potentially huge, ranging from the ubiquitous provisioning of healthcare services to enhanced emergency medical response systems and technologies to promote healthier living styles.

Wearable and implantable medical sensors and devices constitute an already established industry. For example, the market of IMDs has been progressively growing year after year and it is expected to be worth more than $43 billion in 2011 and more than $70 billion in 2018, according to a research made by Transparency Market Research [155]. IMDs are usually given as small microchips located inside the human body to perform some medical-related function. The most common include pacemakers, defibrillators, cochlear implants, insulin pumps, and neurostimulators. In their current generation (or in a near future), all of them share a common feature: wireless communication capabilities [127]. Moreover, IMDs have the ability to support and store telemetry data facilitating the remote monitoring of the patient. IMDs can be part of a WBANs, operating both as sensors and as actuators and making decisions in real time.

In recent years, the proliferation of smartphones and other mobile "smart" devices with substantial computational and communication capabilities have reshaped the

way WBANs may be implemented. Many works put a smartphone as WBAN central node, using Bluetooth and Wi-Fi connections to group together all wearable sensors and devices. Apps running on the smartphone and other smart wearable devices provide an interface to access sensor data, which can be forwarded to healthcare staff using the smartphone Internet connection. Offloading computing and storage capabilities to the cloud has also been suggested to overcome the limitations of wearable devices [31, 107]

Security and privacy issues have been described as two of the most challenging problems of IMDs and, more generally, WBANs [6, 47, 84, 103]. As an example, it has been demonstrated that somebody equipped with a low cost device can eavesdrop on the data communicated with a pacemaker and may even induce a cardiac arrest [71]. Health-related data have been the focus of several attacks almost since the adoption of computers in the healthcare domain. The most important security and privacy challenges in WBANs for healthcare scenarios include:

- **Data confidentiality**. Data generated in the WBAN is highly sensitive and must be encrypted both at storage and during transmission, so that users without the appropriate keys cannot access the data [34, 142].
- **Data integrity and authentication**. It must be ensured that a message has been generated by a valid sensor and that it has not been tampered with by an adversary. Data integrity and authentication can be attained using standard cryptographic techniques in WBANs [34, 103, 142].
- **Fine-grained access control**. In this context, fine-grained refers to the granularity of the data access policy defined to specify and enforce different access privileges for different users. Trade-offs between access control and efficiency/usability must be considered, as a higher level of privacy discloses less information but incurs more costs while a lower privacy level leaks more details but may be efficient [70, 103, 178].
- **Software security**. Code running in medical devices should be carefully designed and analysed [34]. Software vulnerabilities in a WBAN sensor or actuator may have serious consequences for the patient's privacy and, in some cases, even lead to life-threatening situations.
- **Limited capabilities**. Most implantable and wearable devices are battery-operated and suffer from severe restrictions in their computing and communication capabilities. Thus, while many traditional embedded systems can rely on cryptographic measures without limitations, this must be carefully considered for implantable and wearable medical devices [47, 103].
- **Realistic threat and operation models**. Currently there are not clearly established models for the typical operation mode of a WBAN and the associated threat model(s). For example, it seems clear that a compromise of one WBAN node (*e.g.*, if it is lost or stolen) should not put at risk other data or devices [34, 103], but more comprehensive security models are needed. Similarly, it is unclear how to manage critical medical situations in which unauthorized users (*e.g.*, paramedics, doctors belonging to a foreign hospital, etc.) can detect the presence of medical devices, get immediate access to them, and even be able to switch them off or reconfigure them [47]. How to efficiently and securely deal with this is still an open problem.

- **Availability**. Sensory data and wearable medical services must be available at all times. More importantly, data and services should be able to dynamically adapt to contexts, such as time, location, or certain events related to patients, and this data should be correct even under Byzantine node failure [103, 142].

4.1.1 Contribution and Organization

In this chapter, we introduce a WBAN architecture based on the publish-subscribe messaging paradigm for wearable and implantable sensors and devices. The WBAN is thus viewed as a shared bus where a number of entities sensors, apps residing in wearable smart devices, external users, etc. produce data and subscribe to the data feed provided by another entities. We present two protocols for publishing data and sending commands to a sensor that guarantee confidentiality and fine-grained access control. Our protocols are based on a recently proposed CP-ABE scheme that is lightweight enough to be embedded into wearable sensors [69].

Contrarily to other WBAN papers based on CP-ABE schemes, in our architecture sensors can encrypt data but also decrypt messages generated by other devices. This allows for a flexible, scalable, and highly versatile architecture where services can be dynamically composed by subscribing to the data feeds published by wearable sensors. One major restriction of our chosen CP-ABE scheme is that only AND-based policies can be formed. Nonetheless, we show that this suffices to implement Lattice-Based Access Control (LBAC) [147] policies, which are highly appropriate for the e-health domain.

The rest of this chapter is organized as follows. In subsection 4.2 we provide some background on ABE techniques and, in particular, on CP-ABE. Our proposed solution is described in subsection 4.3 and evaluated in subsection 4.4, both in terms of security and experimental efficiency. Subsection 4.5 provides an overview of related work in WBAN for healthcare applications. Finally, subsection 4.6 concludes the chapter and discusses our ongoing and future work in this area.

4.2 Preliminaries

For completeness and readability, we next provide a brief overview of the cryptographic primitives used in the protocols proposed in this chapter.

4.2.1 Attribute Based Encryption

ABE was firstly presented by Sahai and Waters in [145] as a new way to provide authenticated users with encrypted access control. ABE is a type of public cryptography technique where messages are encrypted with both a private key and a ciphertext that correspond to the user's public attributes. Data can be decrypted by everyone whose attributes satisfy the policy set by the encryptor. Traditionally, the cost of these schemes in terms of computation, private key size, and ciphertext size increases exponentially with the number of the attributes used. However, recent advances have demonstrated that even some lightweight devices such as RFID labels can implement ABE decryption [69]. Additionally, ABE cryptography is one

of the most suitable cryptographic way to provide access control while having low computation and storage overhead [103].

ABE schemes can be categorized in four different types:

- **Key-Policy Attribute Based Encryption (KP-ABE)**, proposed by Goyal *et al.* [66] in 2006 to achieve fine-grained access control in a more flexible manner than ABE schemes. KP-ABE introduces more complex access structures (policies) to encrypt messages: boolean formula including AND and OR operations. Additionally, each decryption key is based on a set of public attributes S. Finally, a user who wants to decrypt a message must match her attributes with the ciphertext. This is a disadvantage because the owner cannot choose who is able to decrypt messages.
- **Non-monotonic ABE** was proposed by Ostrovsky *et al.* [125] in 2007. In this work, the authors extended the traditional ABE scheme by introducing a boolean formula where AND, OR, NOT, and threshold operations are available. The scheme has overhead problems because of negative clauses, which make it infeasible to be developed in constrained devices.
- **CP-ABE** was proposed by Bethencourt *et al.* [24] in 2007. The authors presented an ABE scheme that corrects one of the disadvantages of KP-ABE, namely the ability of choosing who will be able to decrypt messages. To do so, the authors switch encryption and decryption algorithms, including the attribute set S into the ciphertext and a policy into the key. With this change, the ciphertext is encrypted with a tree access policy and users who want to decrypt a message must match a set of attributes. The scheme's main disadvantage is a high computational cost in the decryption algorithm, particularly if S is large since the more attributes the policy has, the higher the tree is.
- **Hierarchical Attribute-Based Encryption (HABE)** was proposed by Wang *et al.* [158] in 2011 and uses policies in disjunctive normal form, where disjunctions are used to express the access control policy and conjunctions are used to manage all attributes. The scheme does not allow to define fine-grained access control policies, but this can be achieved by combining both Hierarchical Identity-Based Encryption (HIBE) and CP-ABE. HABE is unsuitable to be implemented in real systems because it is assumed that all attributes in one conjunctive clause may be managed by the same authority, which may cause that the same attribute could be managed by multiple authorities.

In 2011, Waters developed a general method to construct a CP-ABE scheme using linear secret sharing techniques [160]. This is the most efficient scheme to date. Additionally, in order to solve the high computational cost that decryption involves, Green *et al.* [67] proposed to offload ABE decryption (KP-ABE and CP-ABE) to an external cloud server. To do so, the authors transform an ABE ciphertext satisfied by a particular set of user attributes into a constant-size ciphertext.

In our work, we rely on CP-ABE schemes because of two main reasons: (i) it is the most suitable option when there are computational constraints [69, 160]; (and ii) the party who encrypts the message chooses who can access the data [24].

4.2.2 CP-ABE Definitions

We next provide a brief background on CP-ABE schemes. We first introduce the notion of access structure, then describe bilinear maps and the variation of the Diffie-Hellman's algorithm known as augmented Multi-Sequence of Exponents Decisional Diffie-Hellman (aMSE-DDH) used in this work, and finally discuss the security model of CP-ABE.

4.2.2.1 Access Structure

We denote by $\mathbb{U}$ the attribute universe description and by $\mathbb{A}$ a collection of attributes $\mathbb{A}_1, \mathbb{A}_2, \ldots, \mathbb{A}_n$, with $A_i \in \{0, 1\}$. $\mathbb{A}$ is an access structure over $\mathbb{U}$ given by a collection of non-empty subsets of $\mathbb{U}$, where the sets specified by $\mathbb{A}$ are called the authorized set. Each time a user joins the system, a list of attributes is assigned to him, implicitly indicating what privileges he will have in the system.

4.2.2.2 Bilinear Pairings

Definition 1. *Let p, r be two different primes, G an elliptic group, g a generator of G, and e a bilinear map: $e : G \times G \to G$ with the next properties:*

- *Bilinear: $\forall u, v \in G$ and $a, b \in \mathbb{Z}_p$ we have $e(u^a, v^b) = e(u, v)^{ab}$.*
- *Non-degenerate: $e(g, g) \neq 1$*
- *Efficient: there exists an efficient algorithm to calculate $e(u, v) \forall u, v \in G$*
- *Symmetric: e is symmetric since $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$*

4.2.2.3 aMSE-DDH

The aMSE-DDH problem is a slight modification of the multi-sequence of exponents decisional Diffie-Hellman problem considered in [48].

Definition 2. *Let x, y, z be three integers. As demonstrated in [74], for any probabilistic algorithm $\mathbb{B}$ making at most n queries using bilinear groups of prime order p, the advantage in solving the aMSE-DDH problem is:*

$$Adv_{\mathbb{B}}^{(x,y,z)-(aMSE-DDH)}(\lambda) = \frac{(n + 2s + 2)^2 \cdot d}{2p} \tag{4.1}$$

Where $s = 4y + 3x + z + 3$ and $d = max\{2(x + 2), 2(y + 2), 4(y - z) + 10\}$

4.2.3 CP-ABE Algorithms

A CP-ABE scheme implements four polynomial-time algorithms: Setup(), KeyGen(), Encrypt(), and Decrypt(). Additionally, some CP-ABE schemes implement a fifth method, named Delegate(), that is used to give temporal access to a given user who is usually not allowed to access that information.

- Setup$(\lambda, \mathbb{A})$. This method requires as input both a security parameter λ and the number of attributes defined in the system. It outputs two parameters: a public parameter PK and a master key MK.
- KeyGen(MK, S). This method requires as input both the master key MK and a set of attributes S that describe the key. It returns a private key SK.

- $\mathsf{Encrypt}(PK, M, \mathcal{T})$. This method requires as input three values: the public parameters PK, the message M, and the access structure $\mathcal{T}$. The algorithm encrypts M and outputs a ciphertext $C_{\mathcal{T}}$ which will only decrypt if and only if the user's attributes satisfy the access structure. We assume that $\mathcal{T}$ is implicitly included in $C_{\mathcal{T}}$.
- $\mathsf{Decrypt}(PK, C_{\mathcal{T}}, SK)$. This method requires as input three values: the public parameters PK, a ciphertext $C_{\mathcal{T}}$ (with the access policy), and a private key SK for an attribute set. The method returns a decrypted message M only if the set of attributes satisfies the access structure embedded in $C_{\mathcal{T}}$; otherwise, it will return the error symbol $\perp$.
- $\mathsf{Delegate}(SK, \hat{S})$. This method requires as input a secret key SK (associated with a set of attributes S) and another set $\hat{S}$ such that $\hat{S} \subseteq S$. It outputs a private key $\widehat{SK}$ for the set $\hat{S}$.

4.2.4 Security Model

The Chosen-Plaintext Attack (CPA) security model is based on the *IND-sAtt-CPA* game, which is a simulation where the adversary tries to attack an encrypted message without a decryption key whose attributes satisfy the message access policy. The game between an adversary and a challenger is described as follows.

Definition 3. *A CP-ABE scheme is said to be secure against an adaptive CPA if any polynomial-time adversary has only a negligible advantage in the* IND-sAtt-CPA *game, where the advantage is defined to be* $Adv = |Pr[b' = b] - 1|$.

- Setup: The challenger starts the algorithm and runs the $\mathsf{Setup}()$ method to generate a key pair (PK, SK) with a security parameter λ, and sends PK to the adversary.
- Phase 1: For each attribute $A_i \in \mathbb{A}$, the adversary gets its secret key SK_i by making requests to the $\mathsf{KeyGen}()$ method. The adversary cannot ask for a $A_i \notin \mathcal{T}$, where $\mathcal{T}$ is his access structure.
- Challenge: The adversary creates two messages M_0 and M_1 with $len(M_0) = len(M_1)$ and an access structure $\mathcal{P}$. Because this structure cannot be satisfied by any SK_i, the challenger picks a random $r \in \{0, 1\}$ and returns the result (C) of the method $\mathsf{Encrypt}(PK, M_r, \mathcal{P})$.
- Query: The adversary can continue querying the $\mathsf{KeyGen}()$ method with the same restriction as in Phase 1.
- The adversary finally gets a guess for r: $r^* \in \{0, 1\}$ and wins the game if $r^* = r$.

The advantage of an adversary is defined by $Adv = Pr[r^* = r] - \frac{1}{2}$.

Definition 4. *The CP-ABE scheme is fully secure against Chosen-Ciphertext Attack (CCA) (CCA-secure) if all polynomial time adversaries have only a negligible advantage for* λ *in this game,* i.e., $Pr[\mathrm{CP} - \mathrm{ABE}(\lambda, \mathbb{U}) = 1] \leq \frac{1}{2} + negl(\lambda)$

It is worth noting that a CP-ABE scheme has all the properties defined in [101] and can be easily adapted to be secure against selective security by adding an initialization phase where the attacker must declare $\mathbb{A}$ before seeing PK. Additionally, it is secure against CPA (CPA-secure) because calls to $\mathsf{Decrypt}()$ are not allowed in Phases 1 and 2 above.

4.3 Our Solution

We next describe our proposed solution. We first provide and architectural overview and discuss the system model. We next describe the three procedures supported in our scheme: setup, publish, and command protocols.

4.3.1 Architecture and System Model

Our solution considers a Body Area Network (BAN) composed of heterogeneous devices in terms of computational and communications capabilities. We assume that many of them are equipped with sensors that provide a number of physical and physiological parameters of the bearer, such as the Electrocardiogram (ECG), Galvanic Skin Response (GSR), temperature, heart rate, position, etc. Some devices could be "smart", meaning that they can execute third-party apps (*e.g.*, a smartphone or a smartwatch), while others could just be wearable or implantable sensors with limited functionality.

At high level, our BAN uses a publish-subscribe architecture [55]. This is a well-known message-oriented system in which parties (*i.e.*, BAN nodes) can play two different roles: nodes who create new events are called publishers and nodes who consume events are called subscribers. Note that in our model "node" is an application-layer entity and should not be viewed as a physical device. For example, a powerful device with various sensors may support various apps running on it, each one publishing a different sensed signal. Similarly, a device may host several subscribers and no provider (*e.g.*, a portable monitor running various apps that provide the bearer with information about his state).

This architecture presents several advantages. For instance, it makes it possible for one sensor to subscribe to the data feed published by another sensor and produce an output that depends on it. This allows for more complex functions to be embedded into wearable devices. For example, a heart rate sensor could subscribe to a location sensor (*i.e.*, GPS) and provide data correlated to the bearer's speed. Furthermore, it makes possible for a sensor to have access to a signal whenever there is another sensor that publishes it in the BAN. Finally, it provides good scalability and flexibility, allowing dynamic topologies among sensor services and, therefore, very powerful applications based on fusing and processing different signals.

In summary, our WBAN architecture can be seen at three different levels (see Fig. 4.1):

- At the physical and network layer, devices will typically organize in a star topology where each node directly communicates with a network hub. This is the traditional approach in most WBANs, with the network hub being a dedicated network controller or, more recently, a smartphone. For reasons that will be clearer later, it is important that such a WBAN controller has sufficient computational resources. The hub will also act as gateway for accessing external services (*i.e.*, the Internet or other devices in the proximity of the WBAN), and in many cases will also provide storage capabilities to other sensors. This, however, can be delegated to another device.
- At the middleware layer, we refer to "entities" rather than to physical sen-

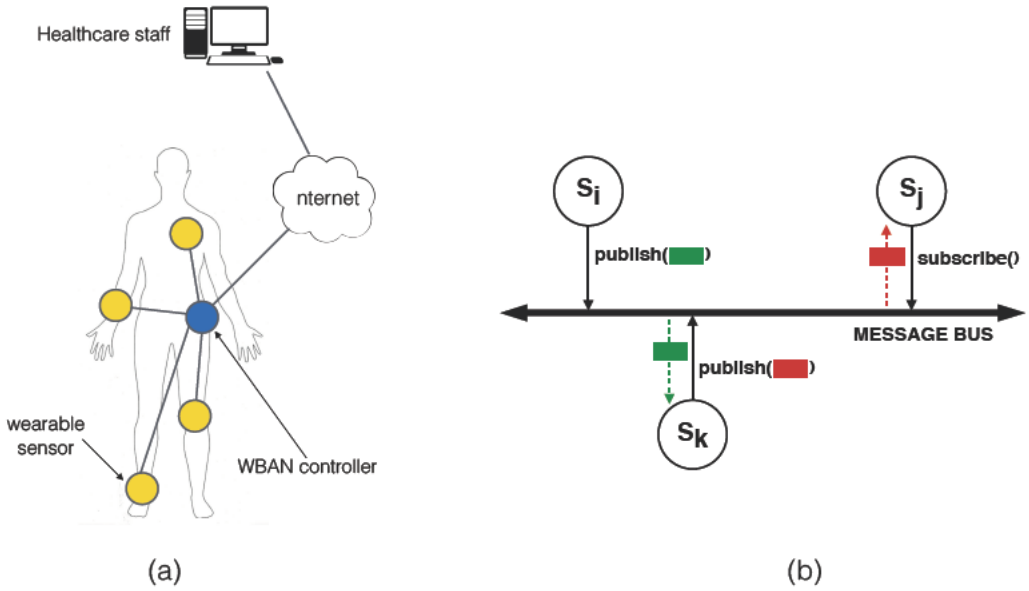


Figure 4.1: WBAN architecture: (a) physically as a network of wearable devices; (b) logically as a publish-subscribe messaging system.

sors or devices. The WBAN is seen as a collection of such entities connected by a (logical) shared bus. The bus is managed by the network hub or any other distinguished element, who provides each entity with a logical view of the architecture through the four classic methods in these architectures [54]: publish(), subscribe(), unsubscribe(), and notify(). Each entity (*e.g.*, a sensor) generates data asynchronously according to its configuration and capabilities. Such data is sent to the bus controller through the publish() method, who stores and forward it to registered subscribers. The particular way in which such transmissions take place depends heavily on the underlying network technologies. For example, if a smartphone plays the role of WBAN controller, one sensor may connect to it using Bluetooth while others may use Wi-Fi.

- Finally, at the application layer we see the WBAN as a collection of sensing services running over different physical nodes. Each service provides a data feed to interested subscribers. Subscribers can be other services running in the WBAN or external entities, such as for example a doctor or a nurse in the case of a medical application. In such a case, access to the WBAN will typically take place through the BAN controller, for example using Internet as communication channel. External entities access services just as a WBAN entity would do it, *i.e.*, using the publish(), subscribe(), unsubscribe(), and notify() methods.

4.3.1.1 Securing Information Flows with Ciphertext Policies

The central aspect of our proposed solution is a fine-grained distributed access control scheme using a lightweight CP-ABE scheme [69]. This is a key security service in healthcare applications of WBANs, since unauthorized access to the data provided by medical sensors may compromise the user's privacy. In our scheme, each

sensor is configured with a policy service that determines what attributes an entity must possess in order to access the data. Such a policy may be fixed (*e.g.*, you need to be a doctor or a nurse to access data published by an ECG sensor) or may depend on the context (*e.g.*, location, state of the patient, readings of other sensors, etc.).

The common approach in WBANs to grant access rights to patient-related data is to follow a Role-Based Access Control (RBAC) model [103]. In a healthcare setting, an RBAC approach classifies users according to their professional roles (*e.g.*, doctors, nurses, admin staff, etc.) and defines policies based on those roles and, perhaps, on external conditions (context) too. CP-ABE supports policies with a tree-like structure, which are adequate to model expressive authorization sentences using roles and context parameters as attributes. Thus, whenever a WBAN sensor generates some data, it builds the ciphertext according to the appropriate access control policy for this particular piece of data.

One major restriction of using the scheme proposed in [69] is that it only supports AND policies. This restricts the types of policies supported in our proposal, although the possibility of having decryption services on-board allows for more complex decision-making since some sensors can decrypt what others publish. Rather than using roles, our current policies are based on LBAC [147]. LBAC is not significantly less expressive than RBAC and fits well the idea of using only AND connectives in the policies. In LBAC, access control policies define a partial order and can be visualized as the Hasse diagram associated with the associated poset. A classical application of such policies is in multilevel security systems, where data is labelled according to its sensitivity level using a number of classification levels (*e.g.*, *public*, *confidential*, *secret*, *top-secret*). Moreover, in order to comply with the need-to-know principle access to information should only be granted if it is necessary for the requester. This gives rise to the use of compartments. In a healthcare scenario, such compartments could correspond to departments or healthcare services.

We will use the following toy example to illustrate the type of LBAC policies supported in our system. Assume a WBAN composed of medical and sport sensors. Medical sensors can be grouped as cardiology-related and neurology-related. The information generated by the sensors belongs to three categories: public (*e.g.*, the heart rate), confidential (*e.g.*, the ECG or the Electroencephalography (EEG)), and sensitive. The combination of these levels and compartments give rise to the Hasse diagram shown in Fig. 4.2. This could be implemented using a set of 5 attributes:

$$\mathbb{A} = \{public, confidential, sensitive, neuro, cardio\}$$

so that each entity (sensors, apps, and users) are provided with a key associated with a subset of $\mathbb{A}$. Note that if a user is given an attribute of level l, he must be also given all attributes corresponding to the levels below.

Additional attributes can be created for specific privileges. For example, the ability to reconfigure a sensor can be explicitly modelled as a separate attribute.

4.3.2 Setup

Each entity (sensor, device, app, etc.) belonging to the WBAN needs to be initialized with the appropriate keys by a Key Generation Center (KGC). The KGC is operated

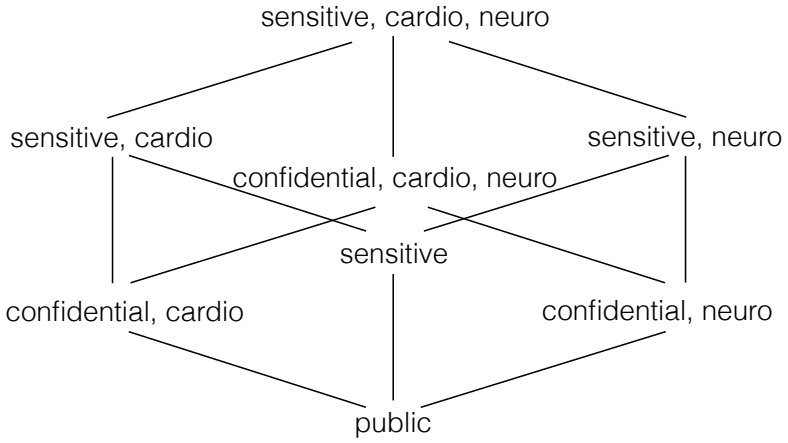


Figure 4.2: Hasse diagram for an example LBAC policy using 3 security levels and 2 compartments.

by the healthcare provider and produces the public parameters PK and a master key MK using the $\mathsf{Setup}(\lambda, \mathbb{A})$ method with policy attributes $\mathbb{A}$. Each entity who wants to join the WBAN must be provided with PK and a secret key SK generated by the KGC using the $\mathsf{KeyGen}(MK, S)$ method, where S is the set of attributes (and, therefore, the access privileges) chosen for the entity.

Once initialized with the appropriate cryptographic material, the entity registers with the WBAN controller and retrieves the list of available sensors (publishers). After this, it can publish it owns contents and subscribe to other sensors' data feeds using the Application Programming Interface (API) provided by the messaging middleware.

4.3.3 Publish Protocol

When a sensor S_i wants to publish data in the data bus, it follows the following procedure:

1. Let d be the piece of data to be published. The sensor S_i must determine under what access policy d will be published. We assume the existence of a policy service stored within the sensor that returns the access structure $\mathcal{A}$ required for this particular piece of data: $\mathcal{A} \leftarrow \mathsf{PubPolicy}(\mathsf{d})$ Note that $\mathsf{PubPolicy}()$ may be as simple as a fixed access policy stored within the sensor, but also arbitrarily complex. For example, a powerful sensor may determine the access structure for a particular piece of data as a function of the location (*e.g.*, whether at home, in the street, at the hospital, etc.), the time of the day, or even the physical state of the bearer. Thus, S_i may need access to external sources of information, including other sensor in the BAN, to determine the context where the publication of d takes place.
2. S_i keeps a list of recently used access structures $\mathcal{A}$ and the associated access token. An access token is just a symmetric key that will be required to actually

get access to d. The list contains the following four elements:

$$[\mathsf{id}(K), \mathcal{A}, \mathsf{Encrypt}(PK_{S_i}, K, \mathcal{A}), t_{\text{exp}}]$$

where:

- $\mathsf{id}(K)$ is the identifier of the access token (symmetric key) K.
- $\mathcal{A}$ is the data structure.
- $\mathsf{Encrypt}(PK_{S_i}, K, \mathcal{A}$ is the CP-ABE encryption of the symmetric key K using $\mathcal{A}$.
- t_{exp} is an expiration date after which this access token is no longer valid.

After determining the access structure $\mathcal{A}$ for this particular d, S_i checks whether a not expired access token is already available. If so, it retrieves it and uses that K in Step 3; otherwise, it creates a new one associated with $\mathcal{A}$ by randomly choosing a symmetric key K. The new access token is sent to the bus so that it becomes available to already subscribed consumers:

$$S_i \rightarrow \text{Bus} : [\mathsf{id}(K), \mathcal{A}, \mathsf{Encrypt}(PK_{S_i}, K, \mathcal{A}), t_{\text{exp}}]$$

3. S_i sends the following message to the bus:

$$S_i \rightarrow \text{Bus} : [S_i, t, \mathsf{id}(K), E_K(d \parallel t)]$$

where:

- S_i is the sensor's identity.
- t is a timestamp.
- $\mathsf{id}(K)$ is the identifier of the access token K.
- $E_K(d \parallel t)$ is the symmetric encryption of d concatenated with t using key K.

4. When a data consumer R who is subscribed to S_i's messages receives a new post, it checks $\mathsf{id}(K)$ and determines whether the corresponding access token is available or not. If this is the first message received with this access structure (*e.g.*, because R has just subscribed to S_i's messages or because S_i has changed the access policy for this piece of data), R must retrieve from S_i the corresponding access token. This is done using the Command Protocol described in the next section. Once retrieved, it executes

$$\mathsf{Decrypt}(PK_R, \mathsf{Encrypt}(PK_{S_i}, K, \mathcal{A}), SK_R)$$

to obtain K (if R has sufficient privileges) and, subsequently, the symmetric decryption $D_K(E_K(d))$ to retrieve d and check t.

The entire protocol is illustrated in Fig. 4.3.

4.3.4 Command Protocol

The Command Protocol implements the "get" and "set" functionalities common in many distributed services. It is used whenever a requester, either a device within the BAN or an external entity, commands a sensor S_i to carry out an action. Such an action may be:

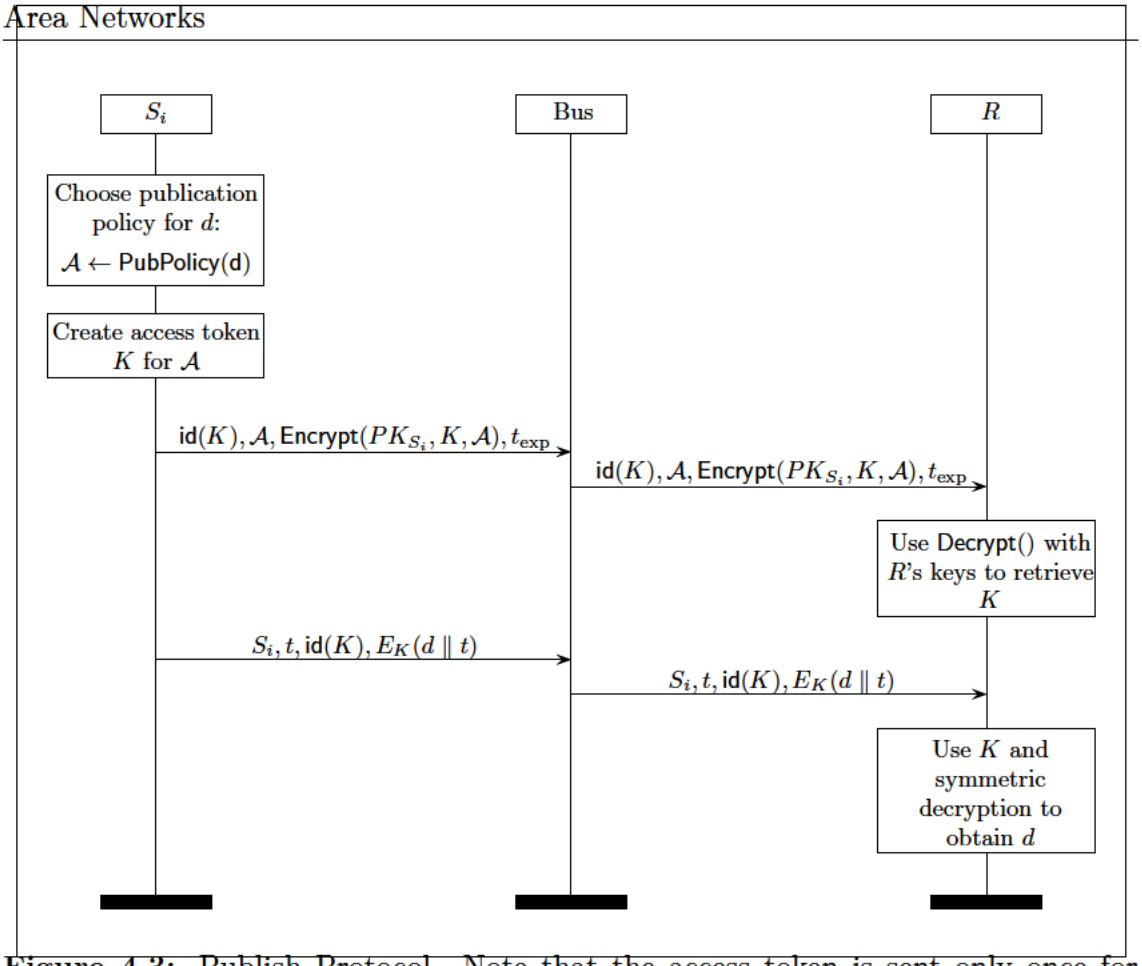


Figure 4.3: Publish Protocol. Note that the access token is sent only once for every access structure.

- A get() command in order to retrieve particular piece of data from the sensor. This could be, for example, the access token required to decrypt S_i's messages. Get operations are also useful to retrieve historical or statistical data stored in the sensor, as well as its configuration in a broad sense.
- A set() command, which is used to modify some configuration aspect of the sensor, including its sensing parameters, network configuration, security policies, etc.

The execution is essentially identical in both cases and consists of the following steps:

1. The requester R selects an appropriate access structure $\mathcal{A}$ and a symmetric key K and sends to the target sensor S_i the message:

$$R \rightarrow S_i : [\mathsf{Encrypt}(PK_R, K_c, \mathcal{A}), E_{K_c}(c \parallel t \parallel R \parallel S_i)]$$

   where c is the get() or set() command with all the associated parameters and t is a timestamp.
2. Upon receiving the previous message, S_i decrypts the first part

$$\mathsf{Decrypt}(PK_{S_i}, \mathsf{Encrypt}(PK_R, K_c, \mathcal{A}), SK_{S_i})$$

   and obtains K_c, which is used to decrypt the second part and get access to c. At this point, and after checking that t and the two identities are correct, S_i

checks whether R has sufficient privileges to require the execution of c. We assume the existence of a command policy service stored in the sensor that returns the privileges (i.e, access structure) $\mathcal{T}$ required to request the execution of c:

$$\mathcal{T} = \mathsf{CmdPolicy(c)}$$

Now, S_i challenges R by sending the message:

$$S_i \rightarrow R : [\mathsf{Encrypt}(PK_{S_i}, (N \parallel t \parallel R \parallel S_i), \mathcal{T})]$$

where N is a nonce.

3. R decrypts the previous message, increases N, and returns:

$$R \rightarrow S_i : [\mathsf{Encrypt}(PK_R, (N+1 \parallel t \parallel R \parallel S_i), \mathcal{T})]$$

4. S_i decrypts the received message and checks that N is correct. If so, it executes c and sends back to R the response $r(c)$ using the same access structure $\mathcal{T}$:

$$S_i \rightarrow R : [\mathsf{Encrypt}(PK, (K_r \parallel t), \mathcal{T}), E_{K_r}(r(c))]$$

In the case of a $\mathsf{get}()$ command, $r(c)$ contains the information requested by R. In the case of a $\mathsf{set}()$ command, $r(c)$ may be a report about the execution or just an ok/error message.

Note that this protocol implicitly assumes that R and S_i can communicate directly, hence the $R \rightarrow S_i$ and $S_i \rightarrow R$ notation. In practice, the WBAN controller will forward the message to the receiver using the appropriate signalling.

The command protocol is illustrated in Fig. 4.4.

4.4 Evaluation

In this section, we discuss the main security properties of the protocols introduced above and report experimental results about their efficiency obtained with a prototype implementation.

4.4.1 Security Analysis

4.4.1.1 Data Confidentiality and Access Control

Confidentiality refers to the protection of sensitive information from being disclosed to unauthorized users. In our solution, we use a hybrid scheme, like the one used in Pretty Good Privacy (PGP), with the aim of guaranteeing confidentiality while offering high efficiency. In the publish protocol presented above, session keys are protected through CP-ABE and then messages are symmetrically encrypted. Therefore, the security guarantees offered by CP-ABE an the strength of symmetric ciphers like AES or 3-DES allow us to claim that our solution do not put at risk confidentiality.

In our solution we offer a fine-grain access control through LBAC polices. Although LBAC is less expressive than RBAC, in Section 4.3.1.1 we have shown how using only AND connectives we are able to define a broad set of policies. In particular, we propose the combined used of security levels and compartments, which helps us to provide wider expressibility despite being limited by using only one operator. On the other hand, the use of compartments suits well the healthcare environment.

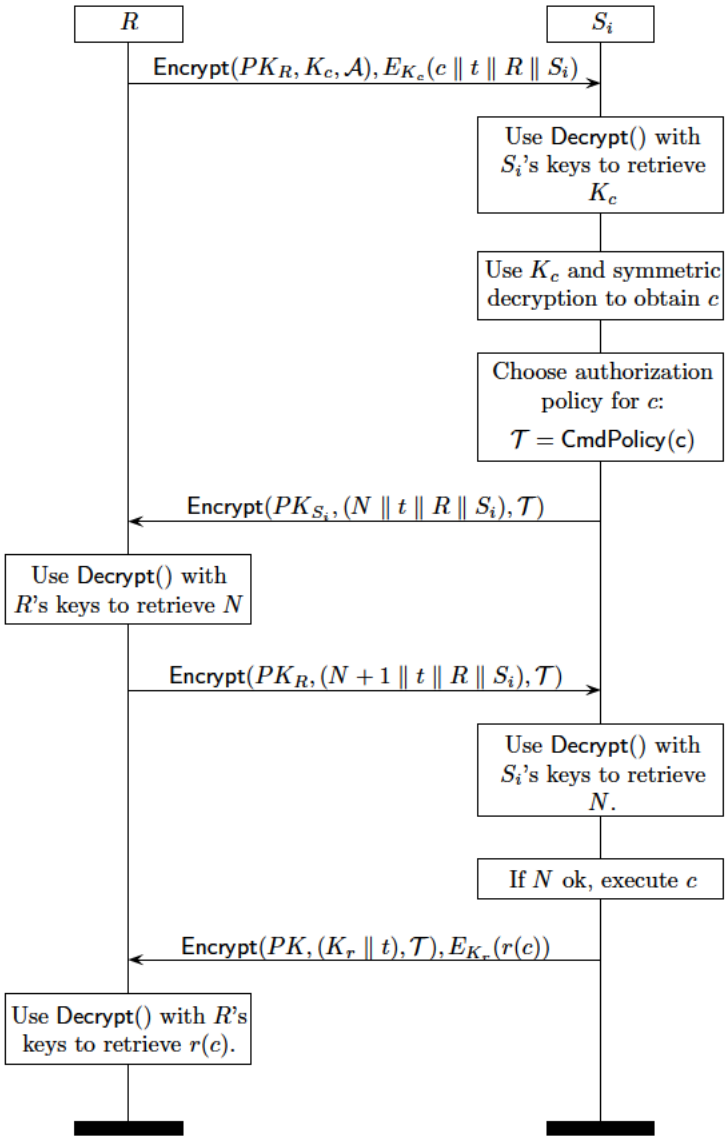


Figure 4.4: Command Protocol

4.4.1.2 Resistance to Collusion Attacks

The use of CP-ABE guarantees resistance against collusion attacks in the following sense: if none of two data subscribers have sufficient privileges to successfully decrypt a ciphertext but the union of their attributes do, it is impossible for them to somehow combine their secret keys to obtain one that can be used to decrypt the ciphertext. The impossibility of doing this is related to the use of different random numbers within each key.

4.4.1.3 Authentication

We have not included authentication tokens neither in the publish protocol nor in in the command protocol. Authentication takes place at the middleware layer, so it is the bus controller in charge of verifying that a publisher is authentic before

accepting a publication. This can be done in a standard way and is not the focus of this chapter.

4.4.1.4 Privacy within the WBAN

Untraceable communications are not one of our design goals in this chapter. Consequently, it is possible for any entity with access to the bus to determine the identity of a sensor, when it publishes something, and even who is subscribed to what service. Avoiding this may be certainly interesting in many scenarios. However, anonymization measures are known to be quite expensive in traditional Wireless Sensor Networks, so lightweight techniques suitable for a WBAN scenario would be welcome.

4.4.2 Performance

We next analyse and evaluate the performance between traditional management and our proposed protocol in terms of functionality, computation, communication and storage overhead.

Comparing both traditional and ABE public key cryptography, one of the major differences they present is related to key distribution. In traditional algorithms, the computation overhead is proportional to the users the system has, *i.e.*, $O(n)$, whereas in CP-ABE schemes the computational overhead usually tends to be $O(1)$. Moreover, there is another main difference between traditional and CP-ABE cryptography in terms of data access: the party who decrypts private data. In traditional system, this operation is made by a trusted party (*e.g.*, the bus controller in our case) before granting access to the final entity and then encrypt the ciphertext with the user's PK. This operation (*encryption + decryption*) increases the system's overhead, whereas in CP-ABE such a trusted party only stores-and-forward data. Decryption will only be made if the user's public attributes match with the access tree included in the ciphertext.

We have developed a prototype of our proposed solution for Android-based devices and run it on a Google Nexus 4 smartphone with a Qualcomm Snapdragon S4 Pro APQ8064 processor and 2GB of RAM. To do this, we built an app that uses a Java implementation of both symmetric encryption/decryption and CP-ABE primitives as in our publish and command protocols. Android v.4.4.4 was used in our tests. In a first round of experiments, we measured the time required by both symmetric and CP-ABE primitives. Fig. 4.5 shows the time required by AES and CP-ABE to encrypt/decrypt 1 MB. The figures were obtained by averaging the result over 10 executions and show that encryption incurs little overhead. In particular, CP-ABE times are quite reasonable considering that in our solution sensors only need to CP-ABE encrypt or decrypt when a new access token is required, which is a relatively infrequent event. Furthermore, access tokens consists basically of an AES key plus some metadata, which amounts to less than 1024 KB. Thus, CP-ABE encryption and decryption of an access token take roughly 3 to 4 ms.

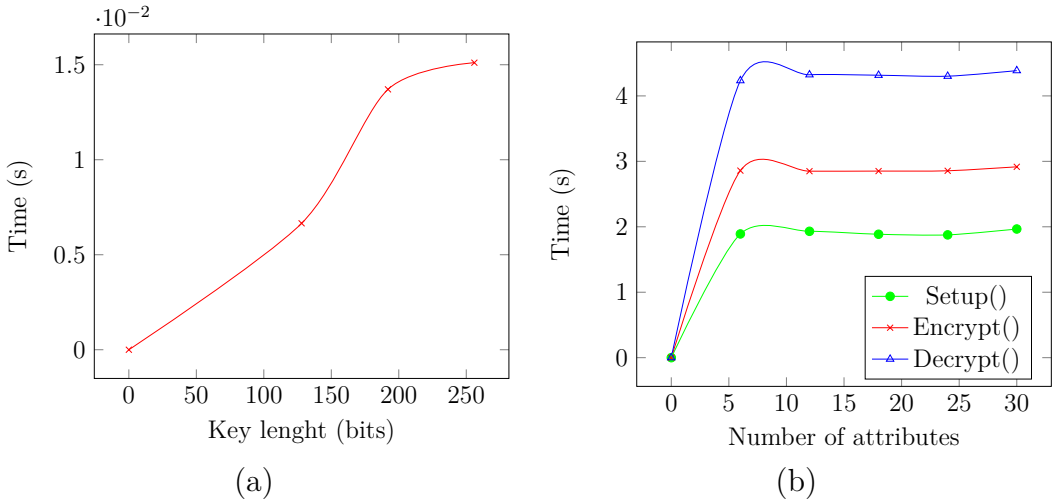


Figure 4.5: Execution time: (a) AES; (b) CP-ABE.

4.4.3 Power Consumption

In battery-powered sensors, power consumption is major limitation and security measures should not be very demanding in this regard. We have also measured the power consumption incurred by our solution when used in an Android platform. The experiments have been conducted by applying a battery of tests involving key generation, encryption, and decryption operations. Our device was previously instrumented with AppScope [176], an energy metering framework based on monitoring kernel activity for Android. AppScope collects usage information from the monitored device and estimates the consumption of each running application using an energy model given by DevScope [88]. AppScope provides the amount of energy consumed by an app in the form of several time series, each one associated with a component of the device (CPU, Wi-Fi, cellular, touchscreen, etc.). We restrict our measures to CPU for computations, as our tests do not have a graphical user interface, do not require user interaction and, therefore, do not use any other component (see Fig. 4.6).

Table 4.1 shows the results in terms of Joules per byte consumed by symmetric and CP-ABE encryption/decryption. As before, the figures are averages obtained over 10 executions. A noteworthy result is that CP-ABE operations are around 1000 times more costly than their symmetric counterpart. This is reasonable and motivates designs like ours in which CP-ABE is only used to encrypt a symmetric key. In order to contextualize the energy implications of the previous figures, we have measured the power consumed by some popular apps during 10 minutes: watching multimedia content in YouTube, playing a game (MX Moto), and online social networking through Facebook (see Table 4.2). The amount of energy consumed ranges between approximately 550 J and 645 J, most of it being related to the graphical user interface.

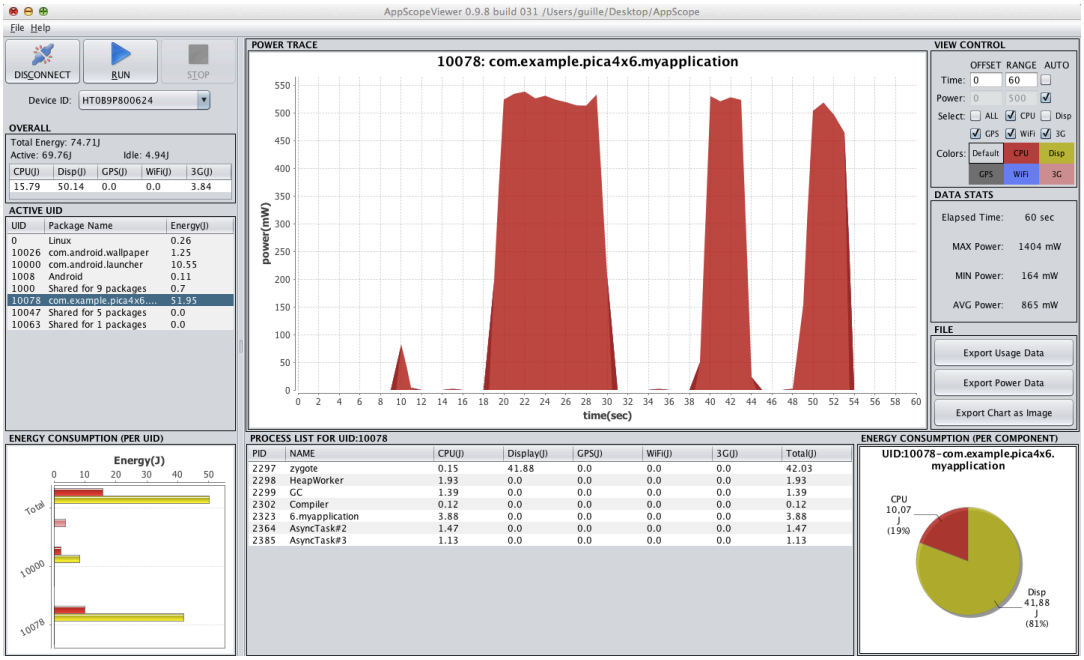


Figure 4.6: Power consumption trace of the CP-ABE Setup(), KeyGen(), Encrypt(), and Decrypt() methods in an Android app.

Primitive	Energy per byte
AES-128/CTR/NoPadding Encryption/Decryption	$7.62 \cdot 10^{-9}$
CP-ABE Encryption	$1.32 \cdot 10^{-6}$
CP-ABE Decryption	$1.01 \cdot 10^{-6}$

Table 4.1: Consumption (in Joules per byte) of symmetric and CP-ABE cryptographic primitives.

4.5 Related Work

WBANs can be grouped into two different categories depending on whether they use an external device [3, 31, 63, 167] or not [17, 104, 107, 111, 141, 175]. The main disadvantage of using an external device is that the patient need to wear it at all times. This increases the chances of it being stolen or lost, which could result in a compromise of all personal data stored on it. Thus, many research works have focused on schemes that do not rely on any external device. This architectures present two main challenges: how data is encrypted and how users can access data. The interested reader can find more information about WBANs in [4].

Bourbakis *et al.* have recently proposed in [30] a mobile health platform for secure information exchange in wearable health monitoring systems. The scheme incorporates various biometric authentication systems that are used to grant access to encrypted health data. Thus, the system incorporates authentication, authorization, confidentiality, and integrity services. Contrarily to our approach, the system in [30] is based on symmetric cryptographic primitives.

Barua *et al.* [17] proposed a scheme to control access to a patient's health in-

App	CPU	Comms	Display	Total
YouTube	30.11	12.59	508.90	551.59
MX Moto	129.24	5.75	509.54	644.52
Facebook	137.76	27.42	471.42	637.27

Table 4.2: Consumption (in Joules) of three popular apps during a time span of 10 minutes.

formation using different privacy levels. To do so, the authors use ABE in a rather standard way: privileges are mapped into roles, and roles into ABE access structures. Additionally, a cloud-based storage is used to reduce the cost and to allow data to be online anytime and anywhere. However, data is sent to the hospital server before storing a copy in the cloud. The hospital server becomes a bottleneck in this scheme, and no data is sent to the cloud if the server is down.

A similar protocol was presented by Akinyele *et al.* in [3]. The protocol uses ABE to generate self-protecting EHRs, which can either be stored on cloud servers or on cellphones so that they could be accessed when the health provider is offline. Their solution is based on how personal health records are managed by the patients themselves using their mobile devices. The schemes involves a large number of messages exchanged between users and healthcare systems, and it is required the existence of a single trusted authority that can decrypt all EHRs. This creates a single point of failure, as the entire system would suffer a major privacy breach if this party is compromised.

In [31], the authors describe a prototype of a cloud mobile health monitoring system based on a WBAN and a smartphone. A neural network located as a cloud service is used to determine whether the patient is in danger. The scheme does not take into account the patient's privacy at any point, neither in the WBAN nor in the cloud, which makes it at least questionable that its applicability in real-world scenarios.

Yi *et al.* proposed in [175] a new protocol in which each sensor stores three different keys that are used to authenticate against three different data servers. If a third party wants access to the patient's data, it needs to obtain authorization from those three data servers.

Another work that uses a cloud server to reduce the decryption computation involved in Identity Based Cryptography (IBE) is the cloud-assisted mHealth monitoring system [107]. This scheme consists of four main components: the cloud server, a company which provides the mHealth monitoring service, patients, and a trust authority. As pointed out in [49], this work does not take into account the energy constraints of sensors and the real-time requirements of this kind of applications.

Many recent works have focused on the problem of controlling access to specific data and assigning privileges to authorized users [104, 111, 141, 178]. In [111], a WBAN is proposed to collect a large amount of data generated by medical sensor networks. The system makes use of a scalable cloud-based infrastructure to store and access the generated data in a secure way. In this work, the authors use CP-ABE and symmetric encryption to achieve fine-grained access with low computation

overhead. A similar concept is proposed in [95], although in this work the authors share devices instead of data like in [111].

Another work based on CP-ASBE (which is an improved form of CP-ABE by introducing a recursive set-based structure on attributes associated with user keys) was presented in [141]. In this work, authors proposed a scheme called CRYPE in order to guarantee the security and privacy of patients when somebody access data that has been previously stored in the cloud. Additionally, IBE is used for secure end-to-end communications. It is claimed that this protocol provides confidentiality, role-base access control with user revocation, scalability, flexibility, and prevention of active attacks such as DoS, and chosen ciphertext and plaintext attacks.

Li *et al.* proposed an attribute revocation method for Multi-Authority Attribute Based Encryption (MA-ABE) systems in [104] to reduce the overhead of key management. This means that the system is split in multiple security domains, each of which manages a subset of users. However this scheme has two main issues: (i) It is only suitable for KP-ABE systems [168]; and (ii) It is a must that each patient generates and distributes her own security keys to the authorized users [111].

A work similar to ours is [75], which focuses on securing the communications between BAN sensors and external users using CP-ABE. Contrarily to our publish-subscribe architecture, the work in [75] takes a data-centric approach in which a data sink receives data from all sensors. Furthermore, sensors can only encrypt and, therefore, cannot access data produced by another sensor.

The proliferation of networked WBAN medical devices has stimulated research on efficient architectures for cryptographic services. For example, the work in [151] proposes a system architecture for implantable devices where security and medical functionalities are decoupled by running then onto two separate cores. The CP-ABE cryptosystem used in our work [69] constitutes another example of lightweight scheme designed on-purpose to be embedded on mobile and wearable devices. Other works in this line include the SCAN secure processor [89], which supporting biometric authentication and various symmetric encryption primitives.

4.6 Conclusions

In this chapter, we have introduced a publish-subscribe architecture for WBANs with particular emphasis in medical applications. In this domain, medical sensors producing highly sensitive information will likely coexist with devices intended for other purposes, such as sport or entertainment apps. We leverage the versatility offered by CP-ABE primitives to propose protocols that allow sensors to subscribe to the data feeds published by other sensors. The privileges required to access each particular data are set by the sensor's policy, who can vary them depending on the context. Apps and external users (*e.g.*, healthcare staff) can get access to such data feeds and also reconfigure or request specific data from the sensors provided that they have sufficient privileges to do so. Our implementation of the underlying protocols make use of a recently proposed lightweight CP-ABE scheme. As consequence of this, the entities use a constant size decryption key which is independent of the used attributes. On the other hand, our scheme offers a fine-grained access control through LBAC policies that are limited to using AND operations only. Finally, it

is worth mentioning that the proposed Publish and Command protocols facilitate to model the principal interactions in a WBAN composed of a variable number of devices.

Our experimental results confirm that the scheme is suitable for most current sensors, including ARM-based platforms.

5

Decentralised Ciphertext Attribute-Based Encryption with Keyword Search

5.1 Introduction

E-Health is a modern healthcare system that employs technology to increase patients' experience of healthcare assistance. For example, *ePrescribing* allows patients to access, print and even to electronically transmit prescriptions from doctors to pharmacists, while *Telemedicine* provides physical and psychological remote diagnosis and treatments. Besides multiple advantages, e-Health is affected by inevitable privacy issues related to data storage, processing and analysis [27, 34]. E-Health deployment relies on sensors which can communicate via wireless channels and share healthcare data. The collection of sensors worn on, in or around the human (body with the sole purpose of monitoring biological signals in real-time) generates the so called WBAN. Since sensors are generally resource-constrained devices, the sensitive collected data needs to be stored on an external, usually not fully trusted, database called cloud server.

Recent works [102, 96, 157, 180] have propose to combine ABE and Searchable Encryption (SE) with the two fold aim of storing encrypted data on semi-honest servers and later on letting authorized users perform encrypted keyword queries on encrypted data. The resulting schemes do not require decryption in order to perform keyword-search, and so avoid the server to get any knowledge on the data or on the queries. Although the afore mentioned schemes provide desirable features (the combination of ABE with SE), all proposals are either based on the very limiting assumption that there exists a single Trusted Authority (TA) controlling all the attributes [180, 96, 157], or allow multiple authorities coordinated by a central entity like in [102]. Lewko [100] was the first to remove the TA and proposed a decentralized ABE scheme. In this chapter, we follow Lewko's footprints and provide a new decentralized schema named Decentralized Ciphertext-Policy Attribute Based Searchable Encryption (DCP-ABSE) without TA. More precisely, in our model there is no hierarchy among the authorities.

Table 5.1 depicts a quick comparison between our proposed scheme and other related works on combining attribute-based encryption and searchable encryption.

	no-CA	MA	no-TA	SE	ABE
[157]	X	✓	✓	X	KP-ABE
[96]	✓	X	X	✓	CP-ABE
VABKS [180]	✓	X	X	✓	CP-ABE / KP-ABE
ARMS [102]	X	✓	X	✓	CP-ABE
Lewko [100]	✓	✓	X	X	CP-ABE
our model	✓	✓	✓	✓	CP-ABE

CA: Central Authority, MA: Multiple Authorities, TA: Trusted Authority, SE: Searchable Encryption

Table 5.1: Comparison of ABSE schemes

Our contributions In this work we will use the publish-subscribe scheme presented in [137] as a starting point to solve the aforementioned questions and we will add some extra features. The purpose of this chapter is threefold:

- We solve the DCP-ABE main issues by adapting the original proposal to a Decentralized Ciphertext-Policy Attribute Based Encryption (DCP-ABSE) presented in [100];
- We introduce a new scheme for attribute based encryption with keyword search based on the union of ABE and SE. In our scheme, a user can query data related to a keyword in the form of tokens, the server will return the ciphertexts that match the queried keyword if and only if the access policy of the query satisfies the access policy of the search determined by the data owner. Finally, the correct decryption of the data retrieved by the user is possible only when the user's attributes satisfy the encryption policy stated by the data owner. Our DCP-ABSE scheme let the data owner specify two (possibly different) policies, one for data decryption and one for keyword search.
- We prove our DCP-ABSE scheme to be resilient against a semi-honest-but-curious server.
- We do not lose any of the original properties presented in [137], including that devices need only to decrypt, the publish-subscribe operation to create and access data feeds, or support for LBAC policies.
- We test the performance of our proposed scheme on different devices including smartphones and ARM-based architectures.

To the best of our knowledge, this is the first work which implements a complete solution based on a decentralized attribute based encryption with keyword search in the context of e-Health systems where two different access policies must be satisfied, one to perform the query and another one to decrypt the data stored in the database.

The contributions of this chapter are as follows. Firstly, we present some cryptographic definitions to understand how the architecture works and how it is going to be improved (refer to Section 5.2). Secondly, we sum up the current proposals done in this area (Section 5.3). After that the core of our proposal named Decentralized Ciphertext-Policy Attribute Based Searchable Encryption (refer to Section 5.4) is proposed and the security analysis can be seen in Section 5.5. This chapter ends with the evaluation of the implemented model (refer to Section 5.6) and some

conclusions (refer to Section 5.7).

5.2 Preliminaries

For completeness and readability, this section collects a brief overview of the cryptographic primitives and security assumptions used throughout the chapter.

5.2.1 Access Structure

Let we denote by $\mathbb{U}$ the attribute universe description and by $\mathbb{A}$ a collection of attributes $\mathbb{A}_1, \mathbb{A}_2, \ldots, \mathbb{A}_n$, with $A_i \in \{0, 1\}$. $\mathbb{A}$ is an access structure over $\mathbb{U}$ given by a collection of non-empty subsets of $\mathbb{U}$, where the sets specified by $\mathbb{A}$ are called the authorized sets.

5.2.2 Bilinear Pairings

Let p be a (large) prime number, G be a multiplicative cyclic group order p and g be a generator of G. A bilinear map e is a function $e : G \times G \rightarrow G_T$ satisfying the following properties:

1. Bilinear: $\forall u, v \in G$ and $a, b \in \mathbb{Z}_p$; we have $e(u^a, v^b) = e(u, v)^{ab}$.
2. Non-degenerate: $e(g, g) \neq 1$ (identity element of G_T).
3. Efficient: there exists an efficient algorithm to calculate $e(u, v)$, $\forall u, v \in G$.
4. Symmetric: e is symmetric, *i.e.*, $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$.

The map e is also called bilinear-pairing, as it takes as pair of elements $((u, v) \in G^2)$ and returns a single value $e(u, v) \in G_T$.

5.2.3 Linear Secret-Sharing Schemes

Definition 1. *A Secret Sharing Scheme (SSS)* Π *over a set of parties* $\mathcal{P}$ *is called Linear Secret Sharing Scheme (LSSS) over* $\mathbb{Z}_p$ *if:*

1. *The shares for each party form a vector over* $\mathbb{Z}_p$.
2. *There exists a matrix* A *(called the share-generating matrix for* Π*) where for all* $x = 1, \cdots, l$*, the* $x-th$ *row of* A *is labelled by a party* $\rho(x)$ *(*ρ *is a function from* $\{1, \cdots, l\}$ *to* $\mathcal{P}$*). When we consider the column vector* $\upsilon = (s, r_2, \cdots, r_n)$*, where* $s \in \mathbb{Z}_p$ *is the secret to be shared and* $r2, \cdots, r_n \in \mathbb{Z}_p$ *are randomly chosen, then* $A\upsilon$ *is the vector of* l *shares of the secret* s *according to* Π*. The share* $(A\upsilon)_x$ *belongs to party* $\rho(x)$.

Following the construction given in [100], for the composite order group construction, LSSS matrices over $\mathbb{Z}_N$ are used, where $N = p_1 p_2 p_3$ is a product of three distinct primes. As in the definition above over $\mathbb{Z}_p$, a set S is authorized if the rows of the access matrix A labeled by elements in S have the vector $(1, 0, \cdots, 0)$ in their span modulo N.

5.2.4 Bilinear Diffie-Hellman (BDH) Assumption

Definition 2. *Let G be a group of prime order p and g be a generator where $|p|$ is proportional to the security parameter λ. There exists a negligible function υ such that for any adversary $\mathcal{A}$, given G, p, g, g^a, g^b, g^c and bilinear map e for randomly chosen $a, b, c \in \mathbb{Z}_p$, $\mathcal{A}$ can distinguish $e(g,g)^{abc}$ from $e(g,g)^R$ for random $R \in \mathbb{Z}_p$ with probability at most $\upsilon(\lambda)$.*

5.2.5 Hardness Assumptions.

In what follows, we consider a group G_N of composite order $N = p_1p_2p_3$ (product of three distinct primes), and a group G_{p_1} of order p_1. Furthermore, we will use an efficiently computable, non-degenerate symmetric bilinear map $e : G_{p_1} \times G_{p_1} \leftarrow G_N$.
Problem 1. *Given a bilinear group generator $\mathcal{G}$, define the following distribution:*

$$G = (N = p_1p_2p_3, G, G_T, e) \xleftarrow{\$} G_G,$$
$$g_1 \xleftarrow{\$} G_{p_1}, D = (G, g_1),$$
$$T_1 \xleftarrow{\$} G, T_2 \xleftarrow{\$} G_{p_1}$$

Assumption 1. *We assume the subgroup decision Problem to be hard in the considered groups,* i.e.*, that any efficient computable algorithm, an adversary $\mathcal{A}$ has only negligible advantage in breaking Problem 1:*

$$Adv_{G,\mathcal{A}}(\lambda) := |\mathsf{Prob}[\mathcal{A}(D, T_1) = 1] - \mathsf{Prob}[\mathcal{A}(D, T_2) = 1]| \ .$$

5.3 Background and Related Work

5.3.1 Attribute Based Encryption

Attribute based encryption was firstly presented by Sahai and Waters in [145] as a type of public cryptography technique where messages are encrypted with both a private key and some user's public attributes. On the other hand, decryption can be run by everyone whose attributes satisfy the policy set during encryption. This technique has become nowadays one of the most interesting cryptographic ways to grant access to data [103].

There are four main categories in ABE: 1) KP-ABE [66]; 2) Non-monotonic ABE [125]; 3) HABE [158]; and 4) CP-ABE [24]. In KP-ABE systems, owners are not able to choose who will decrypt messages. Non-monotonic ABE has overhead problems because of negative clauses and thus makes it unfeasible to be deployed in constrained devices. HABE systems are, as far as we know, unsuitable for most current real systems since they assume that all attributes in one conjunctive clause may be managed by the same authority, and therefore the same attribute cannot be managed by multiple authorities. Finally, CP-ABE systems have high computational cost in the decryption algorithm because of the number of public attributes which make the policy tree unmanageable. However, recent advances have demonstrated that even some lightweight devices, such as RFID labels, can implement ABE decryption [69].

5.3.2 Privacy-Preserving Processing and ABE

A central challenge in the last years is to construct access-control protocols that suite resource constrained devices, *i.e.*, that have low computation and storage overhead and ABE cryptography is a real candidate [103]. Classical proposals [100] have a privacy leakage in terms of public attributes: the TA always knows who is joining the network. The main enabler of this leakage of private information is the key generation algorithm in CP-ABE schemes. In the large majority of the proposals, *KeyGen* algorithm is run by a trusted authority, who thus has access to the public attributes of each new entity without any restrictions.

Guo *et al.* [70] proposed PAAS, a Privacy Preserving Attribute-Based Encryption (PP-ABE) scheme based on four different levels of privacy requirements: 1) authenticated users can check the validity of the attributes without compromising the privacy of the users; 2) both the users' credentials and the values of attributes, can be checked; 3) only a set of public attributes are revealed; 4) in this level, only the size of the intersection of both public attributes and the mobile patients are revealed. As has been pointed out in [146], despite solving the privacy issues this protocol suffers from both cost and communication overheads.

Tong *et al.* [154] attempt to solve the privacy-preservation problem on cloud systems based on ABE and Searchable Symmetric Encryption (SSE). Contrarily to our proposal, Tong *et al.*'s protocol employs ABE to encrypt the secret shares used to generate valid signatures instead of encrypting users health data, which is encrypted by using apparently random identifiers to secure index and symmetric cryptography.

To fight against such a privacy leakage, Chase proposed in 2007 a MA-ABE scheme in [38] to reduce the trust on the central authority and allow cooperation between authorities to initialize the system. Later on, Lewko and Waters presented [100] a multi-authority attribute-based scheme called Decentralized Ciphertext Policy Attribute Based Encryption (DCP-ABE) as an improvement of Chase's protocol, where a central authority is not needed and authorities can work independently.

5.3.3 Searchable Encryption

Searchable encryption is a cryptographic primitive that solves the problem of searching over encrypted data without decrypting the ciphertext. There are two different types of searchable encryption. In private-key searchable encryption schemes, both the data and any other additional data structures are encrypted, so that only users with the private key can access it. In the case of public-key searchable encryption, the encryptor can generate trapdoors to test if some words are in the ciphertext.

Public Encryption with Keyword Search (PEKS) was originally proposed by Boneh *et al.* in [29] and it is considered to be the reference scheme in public-key searchable encryption. PEKS allows senders to store encrypted data on a public server where some keywords are encrypted and attached with the receiver's public key. Additionally, the receiver may send a trapdoor to the server, which is another key based on her own private key, to perform keywords queries without revealing anything about the data or the keywords.

The classical PEKS scheme consists of the following algorithms:

- KeyGen(λ): This method takes a security parameter λ and outputs a public/secret key pair A_{pub}, A_{priv}.
- Tag(A_{pub}, W): This method takes A_{pub} and a keyword W as input and outputs a searchable encryption of W, S_W. It is run by the sender.
- Trapdoor(A_{priv}, W): This method takes both A_{priv} and a keyword W as input and outputs a trapdoor T_W. It is run by the receiver.
- Test(A_{pub}, S_W, T_W): This method takes three parameters: A_{pub}, S_W, and T_W as input, and outputs $True$ if the query matches, that is if the given keyword is in the ciphertext and $False$ otherwise.

The main purpose of PEKS is to avoid the honest-but-curious server to be able to learn anything else. However, in the original proposal, a secure channel is needed. For that reason, Baek *et al.* in [16] proposed an efficient secure channel scheme by providing keyword search in the random oracle model. Some time later, Fang *et al.* [56] improved this proposal in avoiding both secure channels and the use of random oracles.

Most of the searchable encryption proposals need the owner to share a secret key with a set of authorized users or to generate a trapdoor [153]. For that reason, a new cryptographic primitive based on ABE and SE, which we name Attribute Based Searchable Encryption (ABSE) has been proposed recently [96, 157]. The main purpose of ABSE protocols is to allow users to establish a policy not only for data access and to perform encrypted queries looking for a given set of keywords over some encrypted data. As a result, no interaction between data and the server is taking place and thus the semi-honest server is not able to find out the searched keywords. Existing ABSE schemes, however, use a different approach than what we propose in this chapter and additionally [96, 157] do not provide any test of the performances of their schemes on resource constrained devices.

Zheng *et al.* have recently proposed a new ABSE scheme called Verifiable Attribute-based Keyword Search (VABKS) [180], where a set of keywords are defined by the owner, linked to the data, and then stored in an external cloud server. When some user wants to search for a given keyword, she has to retrieve both a public key and a private key from the authority to build the token for that keyword. Once the token is generated, the user sends it to the database which will eventually answer with the search result if and only if the user satisfies the access policy contained in the token.

5.4 Decentralized Ciphertext-Policy Attribute Based Searchable Encryption

In this section, we first introduce the architectural model (Section 5.4.1) and an abstract description of our protocol (Section 5.4.2). Finally, we present a thorough definition of our novel DCP-ABSE scheme (Section 5.4.3).

5.4.1 Architecture

We next describe all entities that take part in our model.

Authorities. These are the entities that directly deal with the policy attributes. The main duty of an authority is to associate attributes to keys and distribute the keys to users. We assume that any two different authorities do not share any common attribute (*i.e.*, one attribute belongs to only one authority). On one hand, all authorities collaborate to create the secret and public master keys used later on in the searchable phase. On the other hand, each authority alone generates both the secret and the public keys for a given attribute *possessed* by the authority. The users' keys (one to encrypt the data and the other to encrypt the keywords) are generated by the authorities separately and according to the attributes the user has. In our system, the authorities can be managed by external sources such as hospitals, governments, or private companies. Communications between authorities are assumed to be secure. Furthermore, our model allows any (non-compromised) authority to leave the network at any time without re-initializing the whole system. Similarly, no re-initialization is needed if a new authority joins the system, assuming that there is a secure way to send the (already produced) secret master key to the new authority.

Cloud server. Our model includes an external cloud server where user's data are stored (outsourced). This has become a common setting for multiple beneficial reasons such as reduced costs, improved manageability, high availability, number of sharing resources and/or scalability. The cloud server is considered to be semi-honest (*i.e.*, honest-but-curious) which means that it is assumed to always follow the protocol as specified but tries to learn more information from the protocol execution transcript. The main purpose of the cloud server is to store and allow encrypted queries over the encrypted data.

Users. In our system, users can be classified into two main roles: data owners and common users. As owners, they perform the attribute-based encryption of their own data using their private key. As users, they can perform (attribute-based) queries on the data and decrypt in case the user's attributes satisfy the policy. In our application scenario, users include healthcare staff, researchers, etc., whereas data owners are users with a WBAN who produce, encrypt and send data to the cloud for storage.

5.4.2 Protocol Description

We next present a motivating framework for DCP-ABSE and provide an overview of its algorithms. Figure 5.1 depicts the intended setting for our proposal. The four phases highlighted in Figure 5.1 correspond to the main steps of the protocol:

Phase I (WBAN operation): The data owner has multiple sensors that form the WBAN as well as a hub device (*e.g.*, a smartphone) that acts as WBAN controller. The controller can communicate with the sensors to retrieve the data measured by the sensors using, for example, a protocol such as the one described in [137]. In the following, we will often identify the controller with the data owner.

Phase II (Key distribution): In this phase, the authorities distribute the public keys for each attribute they possess. Moreover, upon the users' request, each

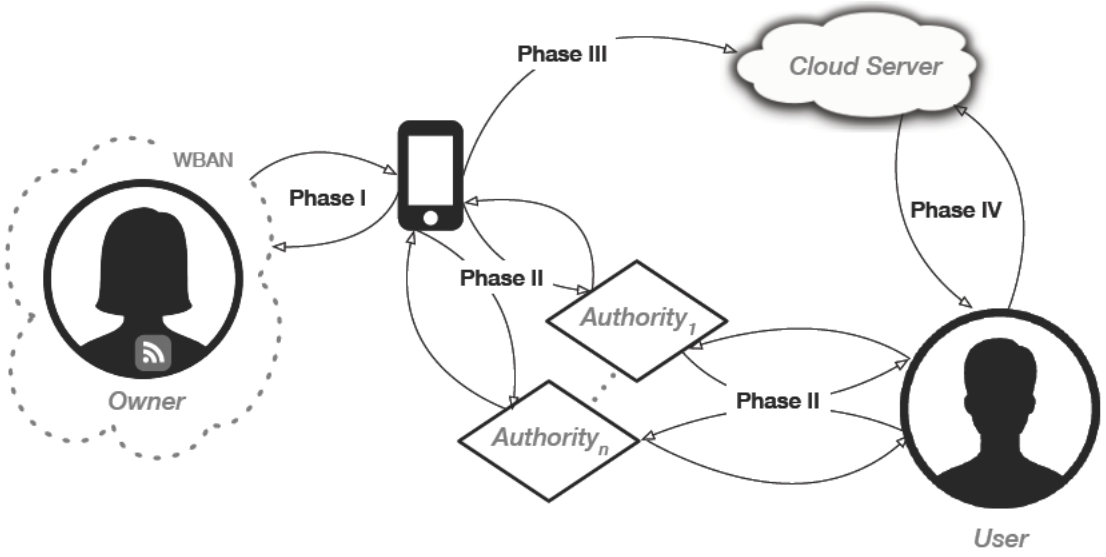


Figure 5.1: Entities in DCP-ABSE.

authority provides a private key for the attributes claimed by the user (data owner).

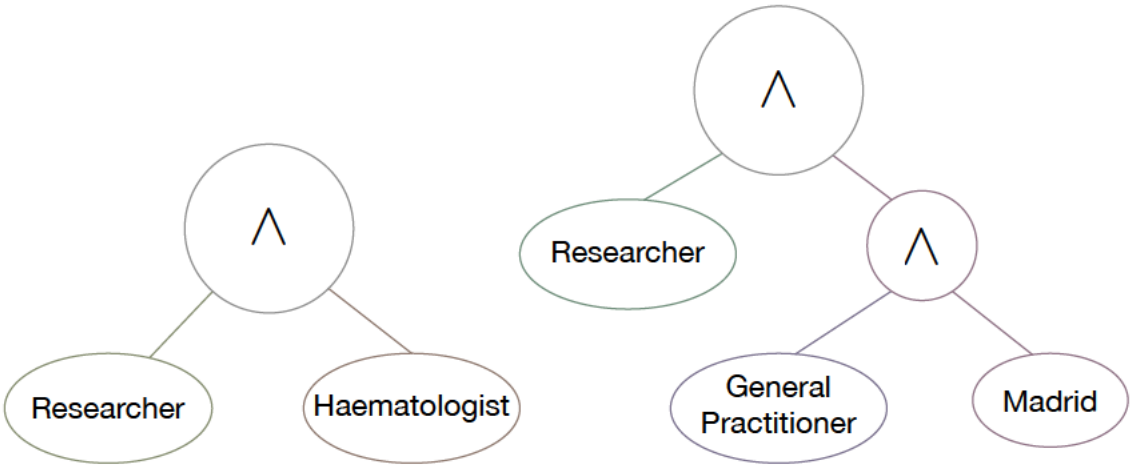
Phase III (Data encryption): The data owner (*i.e.*, controller device) encrypts the data using the keys obtained in Phase II and the desired access policy. In addition, in order to enable other users to search over the encrypted data, the data owner appends to the encrypted data some policy-based keywords. Finally, all the encrypted elements are outsourced to a cloud server.

Phase IV (Keyword search): Using the secret key obtained in Phase II, a user can generate an encrypted query (token) and query the database (cloud server) to identify data that match the query. Upon receiving an answer from the cloud server, the user can decrypt the received data only if she has all the attributes required to satisfy the policy of the encrypted data.

An example of a keyword policy is shown in Figure 5.2. Note that only those users who satisfy the policy can execute queries against the database and retrieve the data they are looking for, but no extra information will be revealed.

We next present a general overview of the methods in DCP-ABSE (see also Figure 5.3 for a diagram of the protocol execution).

- GlobalSetup(λ) $\rightarrow GP$
  This algorithm takes as input the security parameter λ and generates the global parameters, GP, of the public scheme.
- MasterKeyGen(GP) $\rightarrow$ (SMK, PMK)
  Via a Secure Multi-Party Computation (SMPC) protocol, all authorities collaborate in computing a secret master key, SMK (equal for all the authorities), and the corresponding public master key, PMK.
- AuthoritySetup(GP) $\rightarrow$ (SK, PK)
  This algorithm is run by each authority separately. The public key PK and the secret key SK of each authority depend directly on the attributes the authority possesses.



(a) KeyWord: red cells (b) KeyWord: allergies

Figure 5.2: Access policy: (a) Researchers who are haematologists; (b) Researchers who are General Practitioners and live in Madrid.

- KeyGen(GP, SMK, SK, GID, att) $\rightarrow$ ($\text{USK}^{ABE}_{\text{GID},att_i}$, $\text{UMK}^{SE}_{\text{GID}}$)
  Each authority generates the user key, that depends on the user global identity, GID, and the the attribute(s), att, the user possesses.
- Encrypt(GP, PK, (Message, Policy)) $\rightarrow$ C_T
  Using the public parameter and a chosen Policy, the user encrypts the message into a ciphertext (C_T).
- EncyptKeyword(GP, PMK, (Keyword, Policy)) $\rightarrow$ C_{KW}
  With the public parameters the user can encrypt the keyword to be linked to the already encrypted message. The keyword will be encrypted according to a chosen Policy.
- TokenGen(GP, USK, (Query, Policy)) $\rightarrow$ Tkn_{KW}
  The user using the secret key and a policy performs a token for the query (Tkn_{KW}).
- Search(GP, PMK, C_{KW}, Tkn_{KW}) $\rightarrow$ $\{C_T\}$
  This algorithm performs the matching between the encrypted keyword and the token for the query. If the user who computed the token has the correct credentials (satisfies the policy of the keyword), and the query corresponds to the keyword. The final output would be all the data related to the keyword (with the specific policy). Otherwise the result would be null ($\perp$).
- Decrypt(USK, C_T) $\rightarrow$ Message
  This algorithm decrypts the ciphertext given that the user has the appropriate set of attributes. Otherwise it fails.

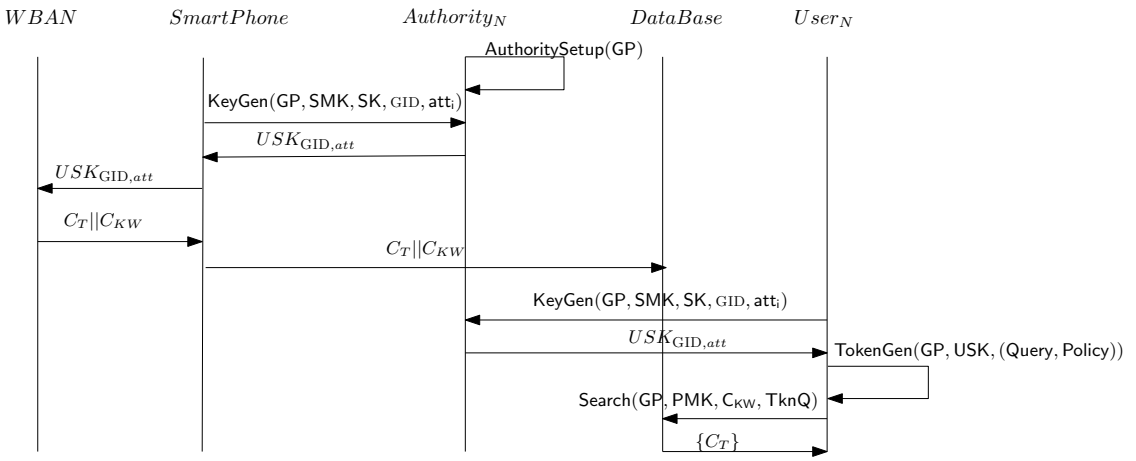


Figure 5.3: Usage of the various subprotocols in DCP-ABSE.

5.4.3 Protocol Design

We describe our proposed scheme CP-ABE that combines ABE and SE in a novel way. More precisely, our protocol enables data-owners to encrypt data under a chosen policy and it also allows users to perform keyword search on the encrypted data in a decentralised context.

- GlobalSetup(λ) $\rightarrow$ GP
  This algorithm takes as input the security parameter λ and uses it to generate a group G_N of composite order $N = p_1p_2p_3$ (satisfying Assumption 1). As a second step, a random element of $G_{p_1} \setminus \{1_{G_{p_1}}\}$ is chosen, namely $g_1 \in G^*_{p_1}$. Eventually the algorithm fixes a bilinear map $e : G_{p_1} \times G_{p_1} \rightarrow G_N$ and three hash functions: $H : \{0,1\}^* \longrightarrow G_{p_1}$, $H_1 : Atts \longrightarrow G_N$ and $H_2 : \{0,1\}^* \longrightarrow \mathbb{Z}_{p_1}$. The set of (public) global parameters is: GP= $\{g_1, N, G_{p_1}, G_N, e, H, H_1, H_2\}$.
- MasterKeyGen(GP) $\rightarrow$ (SMK, PMK)
  This method requires all the authorities of the system to collaborate in a SMPC protocol and jointly generate a pair of master keys (one secret, known to all authorities, and one made public to be used by the users of the system). The algorithm proceeds as follows: each authority $Auth_j$, for $j = 1, \ldots, n$ generates three random numbers $r_j, s_j, t_j \xleftarrow{\$} \mathbb{Z}_{p_1}$. Then the numbers are shared with the other authorities using a SSS, *e.g.*, in order to share r_j, $Auth_j$ elects $n-1$ random numbers $\rho_{j,i} \xleftarrow{\$} \mathbb{Z}_{p_1}$, and sets $\rho_{j,n} = r_j - \sum_{i=1}^{n-1} \rho_{j,i}$. From the shares $\rho_{1,j}, \ldots \rho_{n,j}$, $Auth_j$ can compute the partial result ρ_j and use it (together with the other authorities) to compute the final value $R = \sum_{j=1}^{n} r_j \mod p_1$. Via the same procedure, the authorities can compute $S = \sum_{j=1}^{n} s_j \mod p_1$ and $T = \sum_{j=1}^{n} t_j \mod p_1$. The secret master key is SMK=$\{R, S, T\}$ while the public master key is PMK=$\{g_1^R, g_1^S, g_1^T\}$.
- AuthoritySetup(GP) $\rightarrow$ (SK, PK)
  In this step, each authority generates its own secret key and public key independently from the other authorities. To do so, for each attribute $att_i \in Atts$ belonging to $Auth_j$, it chooses a pair of random numbers $\alpha_i, \beta_i \xleftarrow{\$} \mathbb{Z}_{p_1}$. The public key of authority $Auth_j$ will thus be composed of PK=$\{(e(g_1, g_1)^{\alpha_i}, g_1^{\beta_i}),$

$\forall\ i \in Auth_j\}$ while the secret key will simply be the collection SK=$\{(\alpha_i, \beta_i)$, $\forall\ i \in Auth_j\}$.

- KeyGen(GP, SMK, SK, GID, att_i) $\rightarrow$ ($\text{USK}^{ABE}_{\text{GID},att_i}$, $\text{UMK}^{SE}_{\text{GID}}$)
  The (secret) key for attribute att_i (possessed by the user and by $Auth_j$) is generated as follows. The user provides her Global IDentifier (GID) and the attribute att_i to $Auth_j$. The authority (using the secret key SK) returns to the user two values, $g_1^{\alpha_i} H(\text{GID})^{\beta_i}$ for encryption and $\{g_1^{H_2(\text{GID})} H_1(att_i)^{d_i}, g_1^{d_i}\}$ to perform keywords search. In order for the user to do keyword search, each $Auth_j$ computes $gid = H_2(\text{GID}) \in \mathbb{Z}_{p_1}$, generates random d_i and returns $\text{USK}_{\text{GID},att_i} = \{g_1^{\alpha_i} H(\text{GID})^{\beta_i}, g_1^{gid} H_1(att_i)^{d_i}, g_1^{d_i}\}$ and $\text{UMK}^{SE}_{\text{GID}} = g_1^{\frac{RT-gid}{S}}$, is independent of the attribute and shall be the same for each authority.
- Encrypt(GP, PK, (Message, Policy))$\rightarrow C_T$
  Let $M \in G^n_{p_1}$ be the message (a vector) to be encrypted, and let us represent the Policy as a pair (A, π_A), where A is the $rows(A) \times\ cols(A)$ access matrix, and $\pi_A : \{1, \ldots, rows(A)\} \longrightarrow Atts$ is a function to map the rows of A to attributes. The x-th row of A will be denoted as $A_x \in \{0,1\}^{cols(A)}$. Resembling the scheme in [100], in order to encrypt M according to (A, π_A), the user needs to first construct two random vectors v and w with the following properties. Vector $v = (v_0, \ldots, v_{l-1})^t \xleftarrow{\$} \mathbb{Z}_N^{cols(A)}$ is a random vector, while $w = (0, w_1, \ldots, w_{l-1})^t \in \mathbb{Z}_N^{cols(A)}$ with $w_1, \ldots, w_{l-1} \xleftarrow{\$} \mathbb{Z}_N$. Let υ_x denote $A_x \cdot v \in \mathbb{Z}_N$, similarly let $\omega_x = A_x \cdot w \in \mathbb{Z}_N$. For each row A_x, the user gets a random number $z_x \xleftarrow{\$} \mathbb{Z}_N$. Eventually, the components of the ciphertext are computed as ($\forall x \in \{1, \ldots, rows(A)\}$):

$$\begin{aligned} C_0 &= M \cdot e(g_1, g_1)^{v_0}, \\ C_{1,x} &= \left(e(g_1, g_1)^{\alpha_{\pi_A(x)}}\right)^{z_x} e(g_1, g_1)^{\upsilon_x}, \\ C_{2,x} &= g_1^{z_x}, \\ C_{3,x} &= \left(g_1^{y_{\pi_A(x)}}\right)^{z_x} g_1^{\omega_x} \end{aligned}$$

  and $C_T = \left(C_0, \{C_{1,x}, C_{2,x}, C_{3,x}\}_{x=1}^{rows(A)}\right)$.
- EncyptKeyword(GP,PMK, (Keyword, Policy))$\rightarrow C_{KW}$
  Initially the Keyword is mapped into a group element, using the hash function, *i.e.*, $H(\text{Keyword}) = h \in G_{p_1}$. Then the 'keyword' is encrypted according to the Policy (P, π_p) and the public master key PMK. The following algorithm is an adjustment of Zheng *et al.*'s scheme [180] when the access policy is expressed as an LSSS matrix:
  The user generates two random integers: $a, b \xleftarrow{\$} \mathbb{Z}_{p_1}$. In order to produce shares of b for each row P_x in P ($x = 1, \ldots, rows(P)$) the data owner will pick a random vector $v \in \mathbb{Z}_{p_1}^{cols(P)-1}$ and compute the values $b_x = P_x \cdot (b, v)^t \in \mathbb{Z}_{p_1}$. Finally, the encrypted keyword is produced ($\forall\ x \in \{1, \ldots, rows(P)\}$):

$$\begin{aligned} ckw_1 &= (g_1^T)^a, \\ ckw_2 &= (g_1^R)^{(a+b)} (g_1^S)^{ha}, \\ ckw_3 &= (g_1^S)^b, \\ W_x &= g_1^{b_x}, \\ W'_x &= H_1(\pi_P(x))^{b_x} \end{aligned}$$

and C_{KW}=$\Big(ckw_1$,ckw_2,ckw_3,$\{W_x, W'_x\}_{x=1}^{rows(P)}$, $(P, \pi_P)\Big)$.

- TokenGen(GP,$\text{UMK}^{SE}_{\text{GID}}$, (Query, Policy))$\rightarrow Tkn_{KW}$
  Let Policy=(Q, π) and let $q \in G_{p_1}$ denote the image of the Query$\in \{0,1\}^*$ via the hash function $q = H(\text{Query}) \in G_{p_1}$. The user then picks $rows(Q)+1$ random values $c, d_1, \ldots, d_{rows(Q)} \xleftarrow{\$} \mathbb{Z}_{p_1}$ and generates the token entries as $(\forall x = 1, \ldots, rows(Q))$:

$$\begin{aligned} tok_1 &= ((g_1^R)(g_1^S)^q)^c, \\ tok_2 &= (g_1^T)^c, \\ tok_3 &= (\text{UMK}^{SE}_{\text{GID}})^c, \\ V_x &= (g_1^{gid} H_1(\pi_Q(x))^{d_x})^c, \\ V'_x &= (g_1^{d_x})^c \end{aligned}$$

  The final token is:

$$Tkn_{KW} = \Big(tok_1, tok_2, tok_3, \{V_x, V'_x\}_{x=1}^{rows(Q)}, (Q, \pi_Q)\Big) .$$

- Search(GP,PMK,C_{KW}, Tkn_{KW})$\rightarrow C_T$
  As a first step, Search looks for a subset of attributes $B \subseteq \{\pi_Q(1), \ldots, \pi_Q(rows(Q))\} \subseteq Atts$ that satisfies the policy (P, π_P) present in C_{KW}. If such a B does not exist, Search returns $\perp$. Otherwise, for each attribute $att_x \in B$, it computes $E_{att_x} = \frac{e(V_x, W_x)}{e(V'_x, W'_x)} = e(g_1, g_1)^{b_x\, c\, gid}$. In order to reconstruct the randomness b from the shares b_x, it computes the $|B|$ coefficients $c_x \in \mathbb{Z}_{p_1}$ of the linear combination of rows of Q that satisfies $\sum_x c_x Q_x = (1, 0, \ldots, 0)$. The value b is retrieved via the formula: $\prod_x (E_{att_x})^{c_x} = e(g_1, g_1)^{b\, c\, gid}$. Eventually, Search returns the cihertexts C_T, that are connected to the queried keyword and for which it holds:

$$e(ckw_2, tok_2) = e(ckw_1, tok_1) e(g_1, g_1)^{b\, c\, gid} e(ckw_3, tok_3) .$$

  If there is no data satisfying the previous equality, the algorithm outputs $\perp$.
- Decrypt(GP,$\text{USK}^{ABE}_{\text{GID},att_i}$, C_T)$\rightarrow$ Message
  This method computes $Message \in G_{p_1}$ from C_T. In order for the decryption to work correctly, the user key $\text{USK}^{ABE}_{\text{GID},att_i}$ has to contain the attributes that satisfy the policy under which C_T has been encrypted. The user calculates

$$\frac{C_{1,x} \cdot e(H(\text{GID}), C_{3,x})}{e(\text{USK}_{\text{GID},\pi_A(x)}, C_{2,x})} = e(g_1, g_1)^{\lambda_x} e(H(\text{GID}), g_1)^{\omega_x}$$

  for each $x \in S \subseteq \{1, \ldots, rows(A)\}$, the subset of attribute satisfying the policy (A, π_A). As the user satisfies the policy, then there exist constants $c_x \in \mathbb{Z}_N$ for which $\sum_x c_x A_x = (1, 0, \cdots, 0)$. [1] The values c_x are then used to retrieve v_0 from the shares v_x as follows: $e(g_1, g_1)^{v_0} = \prod_x (e(g_1, g_1)^{v_x} e(H(\text{GID}), g_1)^{\omega_x})^{c_x}$. Finally, $M = C_0 / e(g_1, g_1)^{v_0}$.

[1] The c_x are the coefficient of the linear combination of rows of A that generate (1,0,...,0) and thus satisfy the policy.

Correctness. The decryption of an encrypted message (with matching policies) always returns the plaintext.
It is easy to see that the proposed DCP-ABSE scheme si correct, the proof reduces almost immediately to the correctness of the ABE scheme in [100] and the keyword-search scheme in [180].

Soundness. A user whose attributes do not satisfy the policy of the ciphertext (*resp.* query) shall not be able to decrypt correctly (*resp.* obtain a result other than $\perp$ from Search).
The soundness property follows directly from the soundness of the two base schemes we combine in DCP-ABSE.

5.5 Security Analysis

In this section we first describe the adversary model and the security model for our proposal in Sections 5.5.1 and 5.5.3, respectively.

5.5.1 Adversarial Model

Similarly to the initial schemes [100, 180] we consider an honest-but-curious adversary $\mathcal{A}$ who essentially performs chosen-plaintext attacks. In the games, we do not let $\mathcal{A}$ to corrupt authorities, however our DCP-ABSE scheme is resilient to a static corruption of authorities. The only leakage that comes, is the possibility to generate token queries for any GID of the adversary's choice. We model $\mathcal{A}$ as a Probabilistic Polynomial Time (PPT) algorithm, and define two security games:

1. CPA against message encryption (Game 1)
2. CPA against keyword search (Game 2)

The aim of game 1 is to show that $\mathcal{A}$ cannot exploit keyword search in order to break the ABE scheme used for message encryption. Symmetrically, game 2 captures the scenario in which $\mathcal{A}$ tries to exploit the ABE scheme in order to break the security of the keyword search. After we prove the security for the two games, our model is secure because we can reduce the attacks against DCP-ABSE to attacks against the schemes [100] and [180] separately.

5.5.2 Leakage of Information from Keyword Search on Encrypted Data

In a real world scenario keywords are related to the content of the (plaintext) data returned by Search. For instance, if an attacker produces a token query for the keyword '*blood pressure*', she expects that the returned ciphertext encrypts values between 50 and 200 with high probability. This fact obviously leads to a non-negligible advantage in breaking the semantic security of the ABE encryption scheme. To defend against the leakage of information derived by the keyword search is a direction of independent interests which goes beyond the scope of this chapter. Despite several proposals [16, 56, 62, 149], to the best of the authors' knowledge it is still an open question how to reduce the amount information leaked by searchable encryption schemes in public key scenarios. More precisely, it has been shown [85, 150]

that public-key cryptography alone cannot protect against keyword guessing attacks. Since our DCP-ABSE scheme is built to enable clients to perform keyword search on encrypted data in a public way, we cannot guarantee perfect secrecy for the encryption. Nevertheless, our construction prevents an adversary from deducing any information about the keyword, given keyword ciphertexts (*i.e.*, without allowing any matched search tokens). In other words, we guarantee that $\mathcal{A}$ cannot distinguish the encryption of two keywords, which makes DCP-ABSE search secure against passive adversaries.

5.5.3 Security Model

We define the security for out DCP-ABSE according to the following two games, between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

Game 1 (CPA against message encryption)**.**

Setup The global setup algorithm Setup is run and the output (GP) is used as input in MasterKeyGen method. All public parameters are given to $\mathcal{A}$.

Key Query Phase 1 The adversary makes user key queries to the challenger. More precisely, $\mathcal{A}$ submits queries of the form (att_i, GID) for an attribute att_i and an identity GID (both can variate with the query). The challenger adds the query to a list L (initially empty) and returns the user's key: $(\text{USK}^{ABE}_{\text{GID},att_i}, \text{UMK}^{SE}_{\text{GID}}) \leftarrow KeyGen(SMK, SK, GID, att_i)$.

Challenge Phase The attacker specifies two messages, M_0 and M_1, and two access policies (A, π_A) and (P, π_P). $\mathcal{A}$ can select (P, π_P) freely, while (A, π_A) has to satisfy the following constraint: among the elements in L, for any identity GID, the set of queried attributes att_i shall not satisfy the policy (A, π_A). The challenger then selects a random keyword KW and encrypts it under (P, π_P), obtaining ckw, also $\mathcal{C}$ flips a random coin $\beta \in \{0, 1\}$ and encrypts the message M_β under access matrix (A, π_A). Finally, $\mathcal{C}$ returns to $\mathcal{A}$ the ciphertexts (C_T, ckw).

Query Phase 2 The adversary is allowed to perform keyword queries like in **Phase 1** as long as the pairs (att_i, GID) satisfy the constraints set in the **Challenge Phase**. In addition, $\mathcal{A}$ can perform keyword search queries, by submitting to $\mathcal{C}$ tokens Tkn_{KW}. The challenger runs the Search algorithm and returns to $\mathcal{A}$ the output corresponding to Tkn_{KW}.

Guess The attacker outputs a guess $\beta' \in \{0, 1\}$ for β. $\mathcal{A}$ is said to win the game if $\beta' = \beta$ and the advantage is defined as: $Adv_{CPA+KS}(\mathcal{A}) = |\mathsf{Prob}[\beta' = \beta] - \frac{1}{2}|$.

Note that Game 1 is modified with respect to what would be the standard CPA against DCP-ABSE, in particular we make the challenger choose a *random* keyword to associate to the challenge ciphertext. We have already discussed in 5.5.2 that otherwise we cannot prevent the leakage of some information derived from keyword search.

Theorem 1. *The DCP-ABSE scheme is secure with respect to the CPA against message encryption described in Game 1.*

Proof. We prove that an adversary $\mathcal{A}$ has negligible advantage in Game 1 by showing that the keyword search (in the query phase 2) leaks no useful information to $\mathcal{A}$. Subsequently, we compare $\mathcal{A}$ with an adversary $\mathcal{B}$ involved in the CPA game against

the ABE scheme proposed by Lewko [100]. Since the CPA game in [100] coincides with the Game 1 a part in query phase 2, in as much $\mathcal{A}$ is allowed to perform token queries, it is easy to see that:

$$Adv_{\text{Game 1}}[\mathcal{A}] \leq Adv_{\text{Game in [100]}}[\mathcal{B}] + negl.$$

By the security of Lewko's ABE scheme [100] we have that $Adv_{\text{Game 1}}[\mathcal{A}]$ is negligible. Which proves the statement.

What is left to prove is the initial step: $\mathcal{A}$ gains no considerable advantage by performing keyword search in query phase 2. This is true because of how the challenger picks the keyword to associate to the challenge ciphertext. Since the keyword KW associated to Encrypt(GP, PK, $(M_\beta, (A, \pi_A))$ is chosen at random, a search that matches ckw (the encryption of KW) does not assure that the plaintext of the returned result is somehow related to KW. In query phase 2, if $\mathcal{A}$ submits tokens that do not match ckw the returned result will be $\perp$, so no information is leaked about challenge the ciphertext/plaintex. On the other hand, if the adversary submits a token that matches ckw, $\mathcal{A}$ would receive back the challenge ciphertext C_T. However, KW is independent of the plaintext of C_T by construction, which implies that guessing KW does not give any advantage in breaking the semantic security of the ABE scheme. □

Game 2 (CPA against keyword search)**.**

Setup The global setup algorithm Setup is run and the output (GP) is used as input in MasterKeyGen. All public parameters are given to $\mathcal{A}$.

Key Query Phase 1 The adversary makes user key queries to the challenger. More precisely, $\mathcal{A}$ submits queries of the form (att_i, GID) for an attribute att_i and an identity GID (both can variate with the query). The challenger adds the query to a list L (initially empty) and checks if, for the identity GID, the queried attributes satisfy policy Q^*. If so, $\mathcal{C}$ returns $\perp$, otherwise $\mathcal{C}$ sends to $\mathcal{A}$ the user's key: $(\text{USK}^{ABE}_{\text{GID},att_i}, \text{UMK}^{SE}_{\text{GID}}) \leftarrow KeyGen(SMK, SK, GID, att_i)$.

Challenge Phase The attacker specifies two keywords, KW_0 and KW_1, and an access policy (P, π_P) satisfying the following constraint: among the elements in L, for any identity GID, the set of queried attributes att_i shall not satisfy the policy (P, π_P). The challenger flips two random coins $\alpha, \beta \in \{0, 1\}$ and proceed as follows. First $\mathcal{C}$ produces the challenge encrypted keyword ckw that encrypts KW_β under policy (P, π_P). Then, $\mathcal{C}$ generates a token Tkn from KW_α and the policy (P, π_P) and runs the Search algorithm on the encryption of KW_α under (P, π_P) and Tkn_{KW}. Let C_T denote the result of the Search (*i.e.*, C_T is the ciphertext linked to KW_α under policy (P, π_P)). The challenger returns to $\mathcal{A}$ the encrypted pair (C_T, ckw).

Query Phase 2 The adversary is allowed to perform keyword queries like in **Phase 1** as long as the pairs (att_i, GID) satisfies the constraints set in the **Challenge Phase**. $\mathcal{A}$ can also perform keyword search queries, by submitting to $\mathcal{C}$ tokens Tkn_{KW}. In case Tkn_{KW} is a token for KW_0 or KW_1 (under the policy (P, π_P)), the challenger returns $\perp$, otherwise $\mathcal{C}$ runs Search and returns to $\mathcal{A}$ the output corresponding to Tkn_{KW}.

Guess The attacker outputs a guess $\beta' \in \{0, 1\}$ for β. $\mathcal{A}$ is said to win the game if $\beta' = \beta$ and the advantage is defined as: $Adv_{CKA}(\mathcal{A}) = |\mathsf{Prob}[\beta' = \beta] - \frac{1}{2}|$.

Theorem 2. *The DCP-ABSE scheme is secure with respect to the CPA against keyword search described in Game 2.*

Theorem 2. We prove that an adversary $\mathcal{A}$ has negligible advantage in Game 2 by reducing this game to the Selective Chosen Keyword Attack (SCKA) in [180]. The statement then holds because DCP-ABSE uses Zheng *et al.*'s scheme [180] to perform keyword search.

First, we note that the main difference between Game 2 and SCKA in [180] is that in our case the challenger not only returns the (encrypted) keyword challenge, but also a ciphertext that might be linked to the keyword. This difference let us model the feature of our DCP-ABSE scheme, where both keyword and data coexist. We show that the extra information provided by $\mathcal{C}$ to $\mathcal{A}$ does not increase the adversary's advantage with respect to the SCKA game. Since there is no restriction about the policy with which C_T has been encrypted there are two possible scenarios: (a) $\mathcal{A}$ cannot decrypt C_T, and thus no information is leaked because of the security of the ABE encryption, or (b) $\mathcal{A}$ has queried identities and attributes that satisfy the decryption policy of C_T. In the latter case, however, $\mathcal{A}$ would hold a plaintex that is connect to either KW_0 or KW_1 according to the value of α. Since α is chosen independently from β (which is the bit that $\mathcal{A}$ has to guess) the decryption of C_T does not provide information about the plaintext of ckw. Thus, the advantage of $\mathcal{A}$ in Game 2 is negligibly distant from the advantage of any adversary against the SCKA game. Since the ciphertext-policy keyword-search method used in DCP-ABSE relies on the scheme proposed in [180], and the latter is proven resilient against SCKA, we conclude that our DCP-ABSE is also resilient against keyword attacks.

Alternatively, once clarified that C_T does not influence the adversary advantage, it is straightforward that an adversary $\mathcal{A}$ that wins Game 2 can be used by an adversary $\mathcal{B}$ in the SCKA game to break the security of the Searchable Encryption scheme. □

5.6 Evaluation

The performance of the presented DCP-ABSE scheme is done in three different ways: i) we first evaluate the performance of the master key computation using SMPC; ii) secondly, we isolate each one of the cryptographic operations and compare the computing overhead on different devices; iii) we finally run the whole protocol in a real environment where users can be either a PC or a smartphone.

In all our evaluations we have assumed that the access policy has three attributes connected by an *AND* logical gate, the users have at least four attributes, the type of the curve is "SS512" and the evaluations have been performed taking two different key lengths: 160 and 384 bits [2] while the length of both the encrypted data and the keyword are 130 bytes. Additionally, each one of the tests has been run 10 times and the final running time (given in seconds) is calculated by computing the average time of each one of the partial tests. The SMPC routine used in the experiments is derived from the *Viff*[3] framework implemented in Python and has been deployed

[2] According to the NIST recommendations done in "NIST Special Publication 800-56A"

[3] Virtual Ideal Functionality Framework can be found at http://viff.dk/

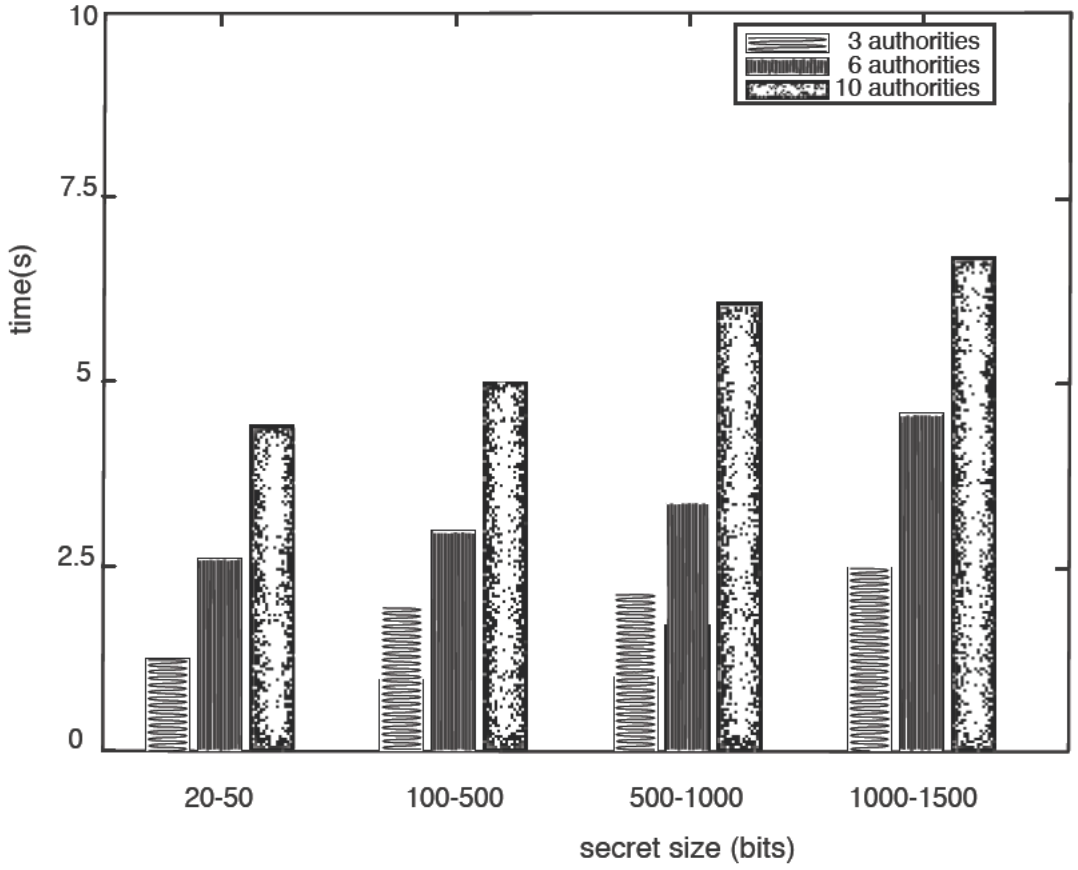


Figure 5.4: Evaluation for the master key generation (SMPC)

on a Debian virtual machine with 1GB and 2 dedicated cores.

The histograms in Figure 5.4 show that the master key generation of our DCP-ABSE scheme (which relies on SMPC) runs within reasonable times when the key size variates from 20 to 1500 bits and the number of authorities involved is either 3, 6 or 10. Additionally, both Table 5.2 and 5.3 show the performance of our proposed model, with a key size that ranges from 160 to 384 bits deployed in both a usual computer and two different smartphones. The data in Figure 5.4 assure that, in the worst tested scenario, our protocol needs about 5 seconds to set up the whole system (with 10 authorities and a secret size between 500 and 1000 bits), *i.e.*, generate the $SMK = \{R, S, T\}$.

In Table 5.2 the performance of the four most common operations can be seen, *i.e.* let g a generator of G so that exponentiations (g^r), pairings $e(g, g)$, multiplications ($g^a \cdot g^b$) and the attribute mapping ($H_1(att)$) are calculated. These operations have been run in three different devices: on a Debian virtual machine (i5 at 2,3 GHz with 1GB RAM and 2 dedicated cores), on a Nexus 4 (Qualcomm Snapdragon S4 Pro at 1,5 GHz with 2GB RAM) and on a Motorola Moto G 3rd Generation (Quad-core 1.4 GHz Cortex-A53 with 2Gb RAM), both of them with the Android 5.1 operation system. In order to perform these experiments we have used the Java Pairing Based Cryptography library (jPBC) for the Android devices and the Charm cryptographic

		g^r	$e(g,g)$	$g^r \cdot g^r$	$H_1(att)$
160 bits	Debian	0.002	0.001	0.003	0.004
	Nexus 4	0.246	0.852	0.474	0.806
	Moto G	0.191	0.433	0.334	0.356
384 bits	Debian	0.005	0.003	0.002	0.010
	Nexus 4	0.740	1.749	1.411	0.334
	Moto G	0.470	0.670	0.743	0.158

Table 5.2: Comparison of performance operations in seconds

		AS	KG	Enc	EKw	Tok	Dec	Search
160 bits	Debian	0.019	0.008	0.033	0.058	0.048	0.016	0.016
	Nexus 4	2.488	3.788	4.360	2.413	5.235	6.694	5.280
	Moto G	1.129	1.549	2.200	1.450	2.921	2.559	2.196
384 bits	Debian	0.041	0.012	0.077	0.087	0.101	0.028	0.037
	Nexus 4	5.649	3.159	9.570	5.501	12.364	10.558	8.937
	Moto G	2.787	1.411	4.912	3.081	6.725	4.896	4.230

Table 5.3: Comparison of DCP-ABSE methods' performance in seconds

framework [2] for the Debian implementation. Results confirm that the heaviest operations when an ABE is used are both pairings ($e(g,g)$) and the H_1 operation (from the attributes set to G_N), however none of the results take more than a second to be run but the Nexus 4 with 384 bits.

Finally, we also provide a time average comparison of the DCP-ABSE methods. In Table 5.3, AuthoritySetup (AS), KeyGen (KG), Encrypt (Enc), EncyptKeyword (EKw), Search (Search), TokenGen (Tok) and Decrypt (Dec) methods are tested. In this case, users can use a either a PC (debian virtual machine) or even a smartphone (Android device). From this analysis, can be seen that even the methods which require more computational resources can be performed by one smartphone in a reasonable time. Furthermore, methods like AuthoritySetup or KeyGen will only be run a few numbers of times to generate and get the keys for the system set up while Search algorithm will usually be run by a back-end server where the database is.

5.7 Conclusions

In this chapter, we have presented DCP-ABSE, a new decentralized attributed based encryption scheme. Our scheme elegantly combines encrypted keyword search and ciphertext policy attribute based encryption. Furthermore, we discussed the security of our scheme and tested its performances on several devices. Our experiments show that all algorithms used by the clients in our DCP-ABSE system can be implemented on highly constrained devices such as smartphones or ARM-based architectures. The running time of the operations required by the algorithms highly depends on the computational power of the chosen device, but in all the cases of study we found acceptable results.

The proposed DCP-ABSE scheme could find interesting applications in e-Health scenarios, as it allows patients to associate multiple keywords to the encrypted data collected by a WBAN. The encrypted data could then be stored in a cloud server together with the encrypted keyword. Subsequently, the healthcare staff could query the server to run a keyword search and retrieve the desired data. Decryption, however, would still depend on the attributes that the staff possesses. Keyword secrecy and Ciphertext secrecy assure the confidentiality of both the query and the stored data.

Three directions that would be interesting to investigate in order to improve our DCP-ABSE are related to (1) the SMPC sub-routine used in the MasterKeyGen, (2) mitigating of the security loss caused by insider attackers and (3) reducing the leakage of information connected to the keyword search.

6

Conclusions

6.1 Summary and Conclusions

This Thesis analyses the security and privacy issues in IoT systems and more precisely in eHealth environments. In the following, the main conclusions that arise from this dissertation are summarized and discussed.

In Chapter 2 it is shown that fingerprint-based authentication protocol proposed in [93] by Jing Huey Khor *et al.* is completely insecure. An attacker, equipped with a domestic PC, can execute a full disclosure attack in only a few minutes. On the other hand, there is not any source of freshness in any of the messages of the protocol, strategy that is often needed to combat replay attacks. Furthermore, de-synchronization of the protocol is simple because the server and the tag only keep the current session key. In fact, there is not any mechanism to recover from a previous state when an incorrect message is received due to errors in the channel or manipulations by an adversary. Therefore, this chapter ruins all the security objectives that the protocol aims to offer. The experimental work carried out leads to the following contributions:

1. Fingerprint$^+$ protocol is presented. The security of this new protocol is formally proven using BAN logic.
2. Fingerprint$^+$ is based on both ISO/IEC 9798-2 and EPC-C1G2 (equivalently ISO/IEC 18000-6C) standards.

In Chapter 3 with the aim of avoiding the use of non-standard constructions that do not follow prudent design practices and established recommendations and informal and/or non-rigorous security analysis, in this chapter, two new RFID protocols for healthcare environments based on standards and international security recommendations (NIST) have been presented. The security of the mechanisms included in these specifications has been deeply studied. The work presented leads to the following conclusions:

1. Details about implementation aspects by following NIST security recommendations are provided to develop new secure authentication protocols.
2. The security schemes proposed are based on (with slightly modifications and tuned for our particular environment) ISO/IEC 9798 and 11770 standards, providing more confidence than ad-hoc designs.

In Chapter 4, a publish-subscribe architecture for WBANs with particular emphasis in medical applications has been presented. In this domain, medical sensors producing highly sensitive information will likely coexist with devices intended for other purposes, such as sport or entertainment apps. The versatility offered by

CP-ABE primitives to propose protocols that allow sensors to subscribe to the data feeds published by other sensors is used. On the other hand, that scheme offers a fine-grained access control through LBAC policies that are limited to AND operators. Finally, it is worth mentioning that the proposed publish and command protocols facilitate to model the principal interactions in a WBAN composed of a variable number of devices. Regarding this work, the next conclusions are stated:

1. The privileges required to access each particular data are set by the sensor's policy, who can vary them depending on the context.
2. Apps and external users (e.g., healthcare staff) can get access to such data feeds and also reconfigure or request specific data from the sensors provided that they have sufficient privileges to do so.
3. The implementation of the underlying protocols make use of a recently proposed lightweight CP-ABE scheme. As consequence of this, the entities use a constant size decryption key which is independent of the used attributes.
4. Experimental results confirm that the scheme is suitable for most current sensors, including ARM-based platforms.

Finally, in Chapter 5 a new decentralized attributed based encryption scheme called Decentralized Cipher-Policy Attribute Based Searchable Encryption that also incorporates keyword search over encrypted data is presented. Contrarily to Lewko's proposal [100] who was the first decentralized ABE schema, we assume that an adversary cannot corrupt authorities but she can make adaptive queries. This assumption is made to prevent attacks against the SMPC algorithm used in the keyword encryption, i.e., if an authority were corrupted then the attacker would have access to a secret master key.

On the one hand, the scheme proposed in [157] requires one central authority to set up the system and multiple authorities are allowed whereas our scheme does not need a central authority. On the other hand, the protocols proposed in [180] and [96] rely on the existence of only one trusted authority controlling all attributes and a recent schema proposed in [102] uses both a central authority and a trusted authority. The main conclusion arisen from this work can be summarized as follows:

1. We solve the DCP-ABE main issues by adapting the original proposal to a Decentralized Ciphertext-Policy Attribute Based Encryption (DCP-ABSE) presented in [100];
2. We introduce a new scheme for attribute based encryption with keyword search based on the union of ABE and SE. Our DCP-ABSE scheme let the data owner specify two (possibly different) policies, one for data decryption and one for keyword search. Both policies must be satisfied in order to retrieve the original information.
3. We prove our DCP-ABSE scheme to be resilient against a semi-honest-but-curious server.
4. We do not lose any of the original properties presented in [137].
5. We test the performance of our proposed scheme on different devices including smartphones and ARM-based architectures.

6.2 Publications

During this PhD, the research work done has resulted in some scientific papers which has been published in scientific journals and in a book chapter. This section describes the published works and the impact or ranking of each of the journals where they have been published.

6.2.1 Publications Related with this Thesis

P. Picazo-Sanchez, L. Ortiz-Martin, P. Peris-Lopez, and J. C. Hernandez-Castro. Security of EPC Class-1. Security and Trends in Wireless Identification and Sensing Platform Tags: Advancements in RFID: Advancements in RFID, page 34, 2012.

P. Picazo-Sanchez, N. Bagheri, P. Peris-Lopez, and J. E. Tapiador. Two RFID standard-based security protocols for healthcare environments. Journal of Medical Systems, 37(5), 2013. IF: 1.372 (Q3-ISI; Q2-SCImago)

P. Picazo-Sanchez, L. Ortiz-Martin, P. Peris-Lopez, and N. Bagheri. Weaknesses of fingerprint-based mutual authentication protocol. Security and Communication Networks, 2014. IF: 0.720 (Q3-ISI; Q2-SCImago)

P. Picazo-Sanchez, J. E. Tapiador, P. Peris-Lopez, and G. Suarez-Tangil. Secure publish-subscribe protocols for heterogeneous medical wireless body area networks. Sensors, 14(12):22619 22642, 2014. IF: 2.245 (Q1-ISI; Q2-SCImago)

6.2.2 Related Publications

P. Picazo-Sanchez, L. Ortiz-Martin, P. Peris-Lopez, J.C. Hernandez-Castro. Cryptanalysis of the RNTS system. The Journal of Supercomputing, 65(2), 949-960. 2013. IF: 0.841 (Q2-ISI; Q3-SCImago)

Bibliography

[1] Cryptographic key length recommendation, May 2015.

[2] J. Akinyele, C. Garman, I. Miers, M. Pagano, M. Rushanan, M. Green, and A. Rubin. Charm: a framework for rapidly prototyping cryptosystems. *Journal of Cryptographic Engineering*, 3(2):111 128, 2013.

[3] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. Peterson, and A. D. Rubin. Securing electronic medical records using attribute-based encryption on mobile devices. In *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, SPSM '11, pages 75 86, New York, NY, USA, 2011. ACM.

[4] M. M. Alam and E. B. Hamida. Surveying wearable human assistive technology for life and safety critical applications: Standards, challenges and opportunities. *Sensors*, 14(5):9153 9209, 2014.

[5] A. Alomainy and Y. Hao. Modeling and characterization of biotelemetric radio channel from ingested implants considering organ contents. *Antennas and Propagation, IEEE Transactions on*, 57(4):999 1005, April 2009.

[6] M. Ameen, J. Liu, and K. Kwak. Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems*, 36(1):93 101, 2012.

[7] A. Arbit, Y. Oren, and A. Wool. Toward practical public key anti-counterfeiting for low-cost epc tags. In *IEEE International Conference on RFID*, pages 184 191, 2011.

[8] J. Aronson. Medication errors: what they are, how they happen, and how to avoid them. *QJM: An International Journal of Medicine*, 102(8):513 521, 2009.

[9] L. Atzori, A. Iera, and G. Morabito. The internet of things: A survey. *Computer Networks*, 54(15):2787 2805, 2010.

[10] AVISPA. Automated Validation of Internet Security Protocols and Applications. Technical report, Avispa, 2005.

[11] G. Avoine. Privacy challenges in rfid. In J. Garcia-Alfaro, G. Navarro-Arribas, N. Cuppens-Boulahia, and S. de Capitani di Vimercati, editors, *Data Privacy Management and Autonomous Spontaneus Security*, volume 7122 of *Lecture Notes in Computer Science*, pages 1 8. Springer Berlin Heidelberg, 2012.

[12] G. Avoine, C. Lauradoux, and T. Martin. When compromised readers meet rfid. In H. Youm and M. Yung, editors, *Information Security Applications*, volume 5932 of *Lecture Notes in Computer Science*, pages 36 50. Springer Berlin Heidelberg, 2009.

[13] S. G. Azevedo and J. J. Ferreira. Radio frequency identification: a case study of healthcare organisations. *Int. J. Secur. Netw.*, 5(2/3):147 155, Mar. 2010.

[14] G. Azuara and J. Salazar. Comprehensive protection of rfid traceability information systems using aggregate signatures. In Á. Herrero and E. Corchado, editors, *Computational Intelligence in Security for Information Systems*, volume 6694 of *Lecture Notes in Computer Science*, pages 168 176. Springer Berlin Heidelberg, 2011.

[15] C. Bachmann, M. Ashouei, V. Pop, M. Vidojkovic, H. Groot, and B. Gyselinckx. Low-power wireless sensor nodes for ubiquitous long-term biomedical signal monitoring. *Communications Magazine, IEEE*, 50(1):20 27, January 2012.

[16] J. Baek, R. Safavi-Naini, and W. Susilo. Public key encryption with keyword search revisited. In O. Gervasi, B. Murgante, A. Laganà, D. Taniar, Y. Mun, and M. Gavrilova, editors, *Computational Science and Its Applications ICCSA 2008*, volume 5072 of *Lecture Notes in Computer Science*, pages 1249 1259. Springer Berlin Heidelberg, 2008.

[17] M. Barua, X. Liang, R. Lu, and X. Shen. Peace: An efficient and secure patient-centric access control scheme for ehealth care system. In *Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on*, pages 970 975, April 2011.

[18] D. Basin and C. Cremers. Evaluation of ISO/IEC 9798 protocols. Technical report, CRYPTREC, 4 2011. Version 2.0.

[19] D. Basin, C. Cremers, and S. Meier. Provably repairing the iso/iec 9798 standard for entity authentication. *Journal of Computer Security*, 21(6):817 846, 2013.

[20] D. Basin, C. Cremers, K. Miyazaki, S. Radomirovic, and D. Watanabe. Improving the security of cryptographic protocol standards. *Security Privacy, IEEE*, PP(99):1 1, 2014.

[21] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede. Public-key cryptography for RFID-Tags. In *Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops*, pages 217 222, 2007.

[22] J. D. Beer. Research note future trends in life expectancies in the european union. *European Commission*, pages 1 17, August 2006.

[23] G. Benelli and A. Pozzebon. Nfcare-possible applications of nfc technology in sanitary environments. In *International Conference on Health Informatics*, pages 58 65, 2009.

[24] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *Security and Privacy, 2007. SP '07. IEEE Symposium on*, pages 321 334, May 2007.

[25] A. Biryukov. Block ciphers and stream ciphers: The state of the art. Cryptology ePrint Archive, Report 2004/094, 2004. http://eprint.iacr.org/.

[26] B. Blanchet. Automatic verification of security protocols in the symbolic model: The verifier proverif. In A. Aldini, J. Lopez, and F. Martinelli, editors, *Foundations of Security Analysis and Design VII*, volume 8604 of *Lecture*

Notes in Computer Science, pages 54 87. Springer International Publishing, 2014.

[27] J. A. Blaya, H. S. Fraser, and B. Holt. E-health technologies show promise in developing countries. *Health Affairs*, 29(2):244 251, 2010.

[28] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe. Present: An ultra-lightweight block cipher. In *Cryptographic Hardware and Embedded Systems - CHES 2007*, volume 4727 of *Lecture Notes in Computer Science*, pages 450 466. Springer Berlin Heidelberg, 2007.

[29] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano. Public key encryption with keyword search. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 506 522. Springer Berlin Heidelberg, 2004.

[30] N. Bourbakis, A. Pantelopoulos, R. Kannavara, and K. Nikita. *Security and Privacy in Biomedical Telemetry: Mobile Health Platform for Secure Information Exchange*, pages 382 418. Wiley-IEEE, 2014.

[31] A. Bourouis, M. Feham, and A. Bouchachia. A new architecture of a ubiquitous health monitoring system: A prototype of cloud mobile health monitoring system. *CoRR*, abs/1205.6910, 2012.

[32] C. Boyd and A. Mathuria. *Protocols for Authentication and Key Establishment*. Springer Publishing Company, Incorporated, 1st edition, 2010.

[33] R. Bunduchi, C. Weisshaar, and A. U. Smart. Mapping the benefits and costs associated with process innovation: The case of rfid adoption. *Technovation*, 31(9):505 521, 2011.

[34] W. Burleson, S. S. Clark, B. Ransford, and K. Fu. Design challenges for secure implantable medical devices. In *Proceedings of the 49th Annual Design Automation Conference*, DAC '12, pages 12 17, New York, NY, USA, 2012. ACM.

[35] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *ACM Trans. Comput. Syst.*, 8(1):18 36, Feb. 1990.

[36] C. Cannière, O. Dunkelman, and M. Knežević. KATAN and KTANTAN — A family of small and efficient hardware-oriented block ciphers. In *Cryptographic Hardware and Embedded Systems - CHES 2009*, volume 5747 of *Lecture Notes in Computer Science*, pages 272 288. Springer Berlin Heidelberg, 2009.

[37] H.-L. Chan, T.-M. Choi, and C.-L. Hui. Rfid versus bar-coding systems: Transactions errors in health care apparel inventory control. *Decision Support Systems*, 54(1):803 811, 2012.

[38] M. Chase. Multi-authority attribute based encryption. In *Proceedings of the 4th Conference on Theory of Cryptography*, TCC'07, pages 515 534, Berlin, Heidelberg, 2007. Springer-Verlag.

[39] C.-L. Chen and Y.-Y. Deng. Conformation of {EPC} class 1 generation 2 standards {RFID} system with mutual authentication and privacy protection. *Engineering Applications of Artificial Intelligence*, 22(8):1284 1291, 2009.

[40] Y.-Y. Chen, D.-C. Huang, M.-L. Tsai, and J.-K. Jan. A design of tamper resistant prescription rfid access control system. *Journal of Medical Systems*, 36(5):2795 2801, 2012.

[41] Y.-Y. Chen, Y.-J. Wang, and J.-K. Jan. A secure 2G-RFID-Sys mechanism for applying to the medical emergency system. *Journal of Medical Systems*, 37(3):1 10, 2013.

[42] X. Cheng, D. Senior, C. Kim, and Y.-K. Yoon. A compact omnidirectional self-packaged patch antenna with complementary split-ring resonator loading for wireless endoscope applications. *Antennas and Wireless Propagation Letters, IEEE*, 10:1532 1535, 2011.

[43] Z.-Y. Cheng, Y. Liu, C.-C. Chang, and S.-C. Chang. Authenticated rfid security mechanism based on chaotic maps. *Security and Communication Networks*, 6(2):247 256, 2013.

[44] H.-Y. Chien. Sasi: A new ultralightweight rfid authentication protocol providing strong authentication and strong integrity. *Dependable and Secure Computing, IEEE Transactions on*, 4(4):337 340, Oct 2007.

[45] H.-Y. Chien and C.-H. Chen. Mutual authentication protocol for rfid conforming to epc class 1 generation 2 standards. *Computer Standards & Interfaces*, 29(2):254 259, 2007.

[46] H.-Y. Chien, C.-C. Yang, T.-C. Wu, and C.-F. Lee. Two rfid-based solutions to enhance inpatient medication safety. *Journal of Medical Systems*, 35(3):369 375, 2011.

[47] A. Darwish and A. E. Hassanien. Wearable and implantable wireless sensor network solutions for healthcare monitoring. *Sensors*, 11(6):5561 5595, 2011.

[48] C. Delerablée and D. Pointcheval. Dynamic threshold public-key encryption. In D. Wagner, editor, *Advances in Cryptology CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 317 334. Springer Berlin Heidelberg, 2008.

[49] O. Diallo, J. J. Rodrigues, M. Sene, and J. Niu. Real-time query processing optimization for cloud-based wireless body area networks. *Information Sciences*, 284(0):84 94, 2014. Special issue on Cloud-assisted Wireless Body Area Networks.

[50] D. N. Duc and K. Kim. Defending rfid authentication protocols against dos attacks. *Computer Communications*, 34(3):384 390, 2011.

[51] P. Dunbar. 300,000 babies stolen from their parents - and sold for adoption: Haunting bbc documentary exposes 50-year scandal of baby trafficking by the catholic church in spain, 2011.

[52] EPC. Class-1 Generation-2 Class-1 Generation 2 UHF Air Interface Protocol Standard Version 1.2.0. Technical report, Global Inc EPC, 2008.

[53] EPC. EPC Radio-Frequency Identity Protocols EPC Class-1 HF RFID Air Interface Protocol for Communications at 13.56 MHz Version 2.0.3. Technical report, Global Inc EPC, 2011.

[54] C. Esposito, D. Cotroneo, and S. Russo. On reliability in publish/subscribe services. *Computer Networks*, 57(5):1318 1343, 2013.

[55] P. T. Eugster, P. A. Felber, R. Guerraoui, and A.-M. Kermarrec. The many faces of publish/subscribe. *ACM Comput. Surv.*, 35(2):114 131, June 2003.

[56] L. Fang, W. Susilo, C. Ge, and J. Wang. Public key encryption with keyword search secure against keyword guessing attacks without random oracle. *Information Sciences*, 238(0):221 241, 2013.

[57] M. Feldhofer and C. Rechberger. A case against currently used hash functions in rfid protocols. In *Proceedings of the 2006 international conference on On the Move to Meaningful Internet Systems - Workshops - Volume Part I*, OTM'06, pages 372 381. Springer-Verlag, 2006.

[58] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen. Aes implementation on a grain of sand. *IEE Proceedings - Information Security*, 152(1):13 20, October 2005.

[59] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Advances in Cryptology - CRYPTO '86, Santa Barbara, California, USA, 1986, Proceedings*, volume 263 of *Lecture Notes in Computer Science*, pages 186 194. Springer, 1986.

[60] K. Fischer and J. Gesner. Security architecture elements for iot enabled automation networks. In *Emerging Technologies Factory Automation (ETFA), 2012 IEEE 17th Conference on*, pages 1 8, Sept 2012.

[61] X. Fu and Y. Guo. A lightweight rfid mutual authentication protocol with ownership transfer. In *Advances in Wireless Sensor Networks*, volume 334 of *Communications in Computer and Information Science*, pages 68 74. Springer Berlin Heidelberg, 2013.

[62] A. Gangaa, N. Somu, and V. S. S. Sriram. A novel methodology to mitigate keyword guessing attack using keyword and signature hash. *Indian Journal of Science and Technology*, 8(16), 2015.

[63] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu. They can hear your heartbeats: Non-invasive security for implantable medical devices. *SIGCOMM Comput. Commun. Rev.*, 41(4):2 13, Aug. 2011.

[64] J. L. Gómez Pardo. Classical ciphers and their cryptanalysis. In *Introduction to Cryptography with Maple*, pages 1 33. Springer Berlin Heidelberg, 2013.

[65] L. Gong, R. Needham, and R. Yahalom. Reasoning about belief in cryptographic protocols. In *Research in Security and Privacy, 1990. Proceedings., 1990 IEEE Computer Society Symposium on*, pages 234 248, May 1990.

[66] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM Conference on Computer and Communications Security*, CCS '06, pages 89 98, New York, NY, USA, 2006. ACM.

[67] M. Green, S. Hohenberger, and B. Waters. Outsourcing the decryption of abe ciphertexts. In *Proceedings of the 20th USENIX Conference on Security*, SEC'11, pages 34 34, Berkeley, CA, USA, 2011. USENIX Association.

[68] L. C. Guillou and J.-J. Quisquater. A paradoxical identity-based signature scheme resulting from zero-knowledge. In *Proceedings on Advances in cryptology*, pages 216 231. Springer-Verlag New York, Inc., 1990.

[69] F. Guo, Y. Mu, W. Susilo, D. Wong, and V. Varadharajan. Cp-abe with constant-size keys for lightweight devices. *Information Forensics and Security, IEEE Transactions on*, 9(5):763 771, May 2014.

[70] L. Guo, C. Zhang, J. Sun, and Y. Fang. Paas: A privacy-preserving attribute-based authentication system for ehealth networks. In *Distributed Computing Systems (ICDCS), 2012 IEEE 32nd International Conference on*, pages 224 233, June 2012.

[71] D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pages 129 142, May 2008.

[72] D. Han and D. Kwon. Vulnerability of an {RFID} authentication protocol conforming to {EPC} class 1 generation 2 standards. $Computer Standards \& Interfaces$, 31(4):648 652, 2009.

[73] M. Hell, T. Johansson, A. Maximov, and W. Meier. A stream cipher proposal: Grain-128. In *IEEE International Symposium on Information Theory*, pages 1614 1618. IEEE, 2006.

[74] J. Herranz, F. Laguillaumie, and C. Ráfols. Constant size ciphertexts in threshold attribute-based encryption. In P. Q. Nguyen and D. Pointcheval, editors, *Public Key Cryptography - PKC 2010*, volume 6056 of *Lecture Notes in Computer Science*, pages 19 34. Springer Berlin Heidelberg, 2010.

[75] C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen. Securing communications between external users and wireless body area networks. In *ACM HotWiSec*, pages 31 36, April 19 2013.

[76] H.-H. Huang and C.-Y. Ku. A rfid grouping proof protocol for medication safety of inpatient. *Journal of Medical Systems*, 33(6):467 474, 2009.

[77] ICAO. Machine readable travel documents part 3. Technical report, International Civil Aviation Organization, 2009.

[78] G. Inc. Google scholar, 2015.

[79] ISO. Information technology security techniques entity authentication part 5: Mechanisms using zero knowledge techniques, iso/iec 9798-5:1999. Technical report, International Organization for Standardization, 1999.

[80] ISO. Information technology security techniques entity authentication part 6: Mechanisms using manual data transfer, iso/iec 9798-6:1999. Technical report, International Organization for Standardization, 1999.

[81] ISO. Information technology security techniques entity authentication part 3: Mechanisms using digital signature techniques, iso/iec 9798-3:1998. Technical report, International Organization for Standardization, 2nd ed., 1998.

[82] ISO. Information technology security techniques entity authentication part 2: Mechanisms using symmetric encipherment algorithms, iso/iec 9798-2:1999. Technical report, International Organization for Standardization, 2nd ed., 1999.

[83] ISO. Information technology security techniques entity authentication part 4: Mechanisms using a cryptographic check function, iso/iec 9798-4:1999. Technical report, International Organization for Standardization, 2nd ed., 1999.

[84] S. Javadi and M. Razzaque. Security and privacy in wireless body area networks for health care applications. In S. Khan and A.-S. Khan Pathan, editors, *Wireless Networks and Security*, Signals and Communication Technology, pages 165 187. Springer Berlin Heidelberg, 2013.

[85] I. R. Jeong, J. O. Kwon, D. Hong, and D. H. Lee. Constructing PEKS schemes secure against keyword guessing attacks is possible? *Computer Communications*, 32(2):394 396, 2009.

[86] A. Juels. RFID Security and Privacy: A Research Survey. *IEEE Journal on Selected Areas in Communications*, 24(2):381 394, February 2006.

[87] A. Juels and S. Weis. Defining strong privacy for rfid. In *Pervasive Computing and Communications Workshops, 2007. PerCom Workshops '07. Fifth Annual IEEE International Conference on*, pages 342 347, March 2007.

[88] W. Jung, C. Kang, C. Yoon, D. Kim, and H. Cha. Devscope: a nonintrusive and online power analysis tool for smartphone hardware components. In *Proceedings of the eighth IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis*, pages 353 362. ACM, 2012.

[89] R. Kannavara, S. Mertoguno, and N. Bourbakis. Scan secure processor and its biometric capabilities. *Journal of Electronic Imaging*, 20(2):023014 023014 11, 2011.

[90] G. Kapoor and S. Piramuthu. Vulnerabilities in chen and deng's {RFID} mutual authentication and privacy protection protocol. *Engineering Applications of Artificial Intelligence*, 24(7):1300 1302, 2011. Infrastructures and Tools for Multiagent Systems.

[91] R. Khan, S. Khan, R. Zaheer, and S. Khan. Future internet: The internet of things architecture, possible applications and key challenges. In *Frontiers of Information Technology (FIT), 2012 10th International Conference on*, pages 257 260, Dec 2012.

[92] B. Khoo. Rfid as an enabler of the internet of things: Issues of security and privacy. In *Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing*, pages 709 712, Oct 2011.

[93] J. Khor, W. Ismail, M. Younis, M. Sulaiman, and M. Rahman. Security problems in an rfid system. *Wireless Personal Communications*, 59(1):17 26, 2011.

[94] P. Kitsos, N. Sklavos, M. Parousi, and A. N. Skodras. A comparative study of hardware architectures for lightweight block ciphers. *Computers & Electrical Engineering*, 38(1):148 160, 2012.

[95] A. Kliem and O. Kao. Cosemed - cooperative and secure medical device cloud. In *e-Health Networking, Applications Services (Healthcom), 2013 IEEE 15th International Conference on*, pages 260 264, Oct 2013.

[96] D. Koo, J. Hur, and H. Yoon. Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage. *Computers & Electrical Engineering*, 39(1):34 46, 2013. Special issue on Recent Advanced Technologies and Theories for Grid and Cloud Computing and Bioengineering.

[97] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy. Smart objects as building blocks for the internet of things. *Internet Computing, IEEE*, 14(1):44 51, Jan 2010.

[98] M. Langheinrich. A survey of rfid privacy approaches. *Personal and Ubiquitous Computing*, 13(6):413 421, 2009.

[99] S. H. Lee, J. Lee, Y. J. Yoon, S. Park, C. Cheon, K. Kim, and S. Nam. A wideband spiral antenna for ingestible capsule endoscope systems: Experimental results in a human phantom and a pig. *Biomedical Engineering, IEEE Transactions on*, 58(6):1734 1741, June 2011.

[100] A. Lewko and B. Waters. Decentralizing attribute-based encryption. In K. Paterson, editor, *Advances in Cryptology EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 568 588. Springer Berlin Heidelberg, 2011.

[101] A. Lewko and B. Waters. New proof methods for attribute-based encryption: Achieving full security through selective techniques. In R. Safavi-Naini and R. Canetti, editors, *Advances in Cryptology CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 180 198. Springer Berlin Heidelberg, 2012.

[102] H. Li, D. Liu, K. Jia, and X. Lin. Achieving authorized and ranked multikeyword search over encrypted cloud data. In *Communications (ICC), 2015 IEEE International Conference on*, pages 7450 7455, June 2015.

[103] M. Li, W. Lou, and K. Ren. Data security and privacy in wireless body area networks. *Wireless Communications, IEEE*, 17(1):51 58, February 2010.

[104] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *Parallel and Distributed Systems, IEEE Transactions on*, 24(1):131 143, Jan 2013.

[105] M. Li and M. Zhuang. An overview of physical layers on wireless body area network. In *Anti-Counterfeiting, Security and Identification (ASID), 2012 International Conference on*, pages 1 5, Aug 2012.

[106] X. Li, J. Ma, Y. Xiong, C. Liu, and W. Wang. An enhanced rfid authentication protocol. *Advanced Science Letters*, 7(1):704 707, 2012-03-30T00:00:00.

[107] H. Lin, J. Shao, C. Zhang, and Y. Fang. Cam: Cloud-assisted privacy preserving mobile health monitoring. *IEEE Transactions on Information Forensics and Security*, 8(6):985 997, 2013.

[108] L. Lin, N. Yu, T. Wang, and C. Zhan. Active rfid based infant security system. In M. Ma, editor, *Communication Systems and Information Technology*, volume 100 of *Lecture Notes in Electrical Engineering*, pages 203 209. Springer Berlin Heidelberg, 2011.

[109] Q. Lin and F. Zhang. Ecc-based grouping-proof rfid for inpatient medication safety. *Journal of Medical Systems*, 36(6):3527 3531, 2012.

[110] H. Liu, M. Bolic, A. Nayak, and I. Stojmenović. Taxonomy and challenges of the integration of rfid and wireless sensor networks. *Network, IEEE*, 22(6):26 35, November 2008.

[111] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal. Secure and scalable cloud-based architecture for e-health wireless sensor networks. In *Computer Communications and Networks (ICCCN), 2012 21st International Conference on*, pages 1 7, July 2012.

[112] B. Malkin. Australia's roman catholic church apologises for forced adoptions, 2011.

[113] Markets and Markets. Nanotechnology in medical devices market by product (biochip, implant materials, medical textiles, wound dressing, cardiac rhythm management devices, hearing aid), application (therapeutic, diagnostic, research) - global forecast to 2019, Mar. 2015.

[114] T. McCue. $117 Billion Market For Internet of Things In Healthcare By 2020. Technical report, Forbes, 2015.

[115] C. Medaglia and A. Serbanati. An overview of privacy and security issues in the internet of things. In D. Giusto, A. Iera, G. Morabito, and L. Atzori, editors, *The Internet of Things*, pages 389 395. Springer New York, 2010.

[116] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot. *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 1st edition, 1996.

[117] A. Mitrokotsa, M. Rieback, and A. Tanenbaum. Classifying rfid attacks and defenses. *Information Systems Frontiers*, 12(5):491 505, 2010.

[118] J. Mora-Gutiérrez, C. Jiménez-Fernández, and M. Valencia-Barrero. *Low Power Implementation of Trivium Stream Cipher*, volume 7606 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2013.

[119] P. Najera, J. Lopez, and R. Roman. Real-time location and inpatient care systems based on passive rfid. *Journal of Network and Computer Applications*, 34(3):980 989, 2011.

[120] NCMEC. Newborn/infant abductions. *National Center for Missing & Exploited Children*, page 1, 2012.

[121] NIST. Recommendation for block cipher modes of operation. methods and techniques, NIST special publication 800-38a. Technical report, National Institute of Standards and Technology, 2001.

[122] NIST. Recommendation for block cipher modes of operation: The CMAC mode for authentication, NIST special publication 800-38b. Technical report, National Institute of Standards and Technology, 2005.

[123] NIST. Recommendation for key derivation using pseudorandom functions (revised), NIST special publication 800-108. Technical report, National Institute of Standards and Technology, 2009.

[124] D. Nyamy and P. Urien. Hip-tag, a new paradigm for the internet of things. In *Consumer Communications and Networking Conference (CCNC), 2011 IEEE*, pages 49 54, Jan 2011.

[125] R. Ostrovsky, A. Sahai, and B. Waters. Attribute-based encryption with non-monotonic access structures. In *Proceedings of the 14th ACM Conference on Computer and Communications Security*, CCS '07, pages 195 203, New York, NY, USA, 2007. ACM.

[126] A. Oztekin, F. M. Pajouh, D. Delen, and L. K. Swim. An rfid network design methodology for asset tracking in healthcare. *Decision Support Systems*, 49(1):100 109, 2010.

[127] D. Panescu. Emerging technologies [wireless communication systems for implantable medical devices]. *Engineering in Medicine and Biology Magazine, IEEE*, 27(2):96 101, March 2008.

[128] A. Pantelopoulos and N. Bourbakis. Prognosis a wearable health-monitoring system for people at risk: Methodology and modeling. *Information Technology in Biomedicine, IEEE Transactions on*, 14(3):613 621, May 2010.

[129] S. Parlak, A. Sarcevic, I. Marsic, and R. S. Burd. Introducing rfid technology in dynamic and time-critical medical settings: Requirements and challenges. *Journal of Biomedical Informatics*, 45(5):958 974, 2012.

[130] M. Pasquet, J. Reynaud, and C. Rosenberger. Secure payment with nfc mobile phone in the smarttouch project. In *Collaborative Technologies and Systems, 2008. CTS 2008. International Symposium on*, pages 121 126, May 2008.

[131] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda. Rfid specification revisited. *The internet of things: From RFID to the next-generation pervasive networked systems*, page 6, 2008.

[132] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Tapiador, and J. C. van der Lubbe. Cryptanalysis of an {EPC} class-1 generation-2 standard compliant authentication protocol. *Engineering Applications of Artificial Intelligence*, 24(6):1061 1069, 2011.

[133] P. Peris-Lopez, A. Orfila, A. Mitrokotsa, and J. C. van der Lubbe. A comprehensive rfid solution to enhance inpatient medication safety. *International Journal of Medical Informatics*, 80(1):13 24, 2011.

[134] P. Picazo-Sanchez, N. Bagheri, P. Peris-Lopez, and J. Tapiador. Two rfid standard-based security protocols for healthcare environments. *Journal of Medical Systems*, 37(5), 2013.

[135] P. Picazo-Sanchez, L. Ortiz-Martin, P. Peris-Lopez, and N. Bagheri. Weaknesses of fingerprint-based mutual authentication protocol. *Security and Communication Networks*, pages n/a n/a, 2014.

[136] P. Picazo-Sanchez, L. Ortiz-Martin, P. Peris-Lopez, and J. C. Hernandez-Castro. Security of epc class-1. *Security and Trends in Wireless Identification and Sensing Platform Tags: Advancements in RFID: Advancements in RFID*, page 34, 2012.

[137] P. Picazo-Sanchez, J. E. Tapiador, P. Peris-Lopez, and G. Suarez-Tangil. Secure publish-subscribe protocols for heterogeneous medical wireless body area networks. *Sensors*, 14(12):22619 22642, 2014.

[138] S. Piramuthu. Rfid mutual authentication protocols. *Decision Support Systems*, 50(2):387 393, 2011.

[139] S. Pritchard. The internet of things is revolutionising the world of sport. Technical report, The Guardian, 2015.

[140] X. Qu, L. T. Simpson, and P. Stanfield. A model for quantifying the value of rfid-enabled equipment tracking in hospitals. *Advanced Engineering Informatics*, 25(1):23 31, 2011.

[141] G. K. Ragesh and K. Baskaran. Crype: Towards cryptographically enforced and privacy enhanced wbans. In *Proceedings of the First International Conference on Security of Internet of Things*, SecurIT '12, pages 204 209, New York, NY, USA, 2012. ACM.

[142] S. K. S. Raja and T. Jebarajan. Level based fault monitoring and security for long range transmission in wban. *International Journal of Computer Applications*, 64(1):1 9, February 2013. Published by Foundation of Computer Science, New York, USA.

[143] R. Roman, P. Najera, and J. Lopez. Securing the internet of things. *Computer*, 44(9):51 58, Sept 2011.

[144] M. Safkhani, N. Bagheri, and M. Naderi. On the designing of a tamper resistant prescription rfid access control system. *Journal of Medical Systems*, 36(6):3995 4004, 2012.

[145] A. Sahai and B. Waters. Fuzzy identity-based encryption. In R. Cramer, editor, *Advances in Cryptology - EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 457 473. Springer Berlin Heidelberg, 2005.

[146] O. Said and A. Tolba. Article: SEAIoT: Scalable E-Health Architecture based on Internet of Things. *International Journal of Computer Applications*, 59(13):44 48, December 2012.

[147] R. S. Sandhu. Lattice-based access control models. *IEEE Computer*, 26(11):9 19, 1993.

[148] C. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4(3):161 174, 1991.

[149] Z.-Y. Shao and B. Yang. On security against the server in designated tester public key encryption with keyword search. *Information Processing Letters*, 115(12):957 961, 2015.

[150] E. Shen, E. Shi, and B. Waters. Predicate privacy in encryption systems. In O. Reingold, editor, *Theory of Cryptography*, volume 5444 of *Lecture Notes in Computer Science*, pages 457 473. Springer Berlin Heidelberg, 2009.

[151] C. Strydis, R. M. Seepers, P. Peris-Lopez, D. Siskos, and I. Sourdis. A system architecture, processor, and communication protocol for secure implants. *ACM Trans. Archit. Code Optim.*, 10(4):57:1 57:23, Dec. 2013.

[152] P. R. Sun, B. H. Wang, and F. Wu. A new method to guard inpatient medication safety by the implementation of rfid. *J. Med. Syst.*, 32(4):327 332, Aug. 2008.

[153] W. Sun, S. Yu, W. Lou, Y. Hou, and H. Li. Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud. In *INFOCOM, 2014 Proceedings IEEE*, pages 226 234, April 2014.

[154] Y. Tong, J. Sun, S. Chow, and P. Li. Cloud-assisted mobile-access of health data with privacy and auditability. *Biomedical and Health Informatics, IEEE Journal of*, 18(2):419 429, March 2014.

[155] Transparency Market Research. Implantable medical devices market (reconstructive joint replacement, spinal implants, cardiovascular implants, dental implants, intraocular lens and breast implants) - u.s. industry analysis, size, share, trends, growth and forecast 2012 - 2018, Jan. 2013.

[156] D. Uckelmann, M. Harrison, and F. Michahelles. An architectural approach towards the future internet of things. In D. Uckelmann, M. Harrison, and F. Michahelles, editors, *Architecting the Internet of Things*, pages 1 24. Springer Berlin Heidelberg, 2011.

[157] B. S. Varsha and P. Suryateja. Using attribute-based encryption with advanced encryption standard for secure and scalable sharing of personal health records in cloud. *International Journal of Computer Science & Information Technologies*, 5(5), 2014.

[158] G. Wang, Q. Liu, and J. Wu. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services. In *Proceedings of the 17th*

ACM Conference on Computer and Communications Security, CCS '10, pages 735 737, New York, NY, USA, 2010. ACM.

[159] R. Want. An introduction to rfid technology. *Pervasive Computing, IEEE*, 5(1):25 33, Jan 2006.

[160] B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, editors, *Public Key Cryptography PKC 2011*, volume 6571 of *Lecture Notes in Computer Science*, pages 53 70. Springer Berlin Heidelberg, 2011.

[161] R. H. Weber. Internet of things new security and privacy challenges. *ComputerLaw&SecurityReview*, 26(1):23 30, 2010.

[162] D. M. West. Improving health care through mobile medical devices and sensors, October 2013.

[163] World Health Organization. Global health observatory data repository - life expectancy, 2014.

[164] Z.-Y. Wu, L. Chen, and J.-C. Wu. A reliable rfid mutual authentication scheme for healthcare environments. *Journal of Medical Systems*, 37:1 9, 2013.

[165] D. Wyld. Preventing the worst case scenario: An analysis of rfid technology and infant protection in hospitals. *The Internet Journal of Healthcare Administration*, 7(1), 2010.

[166] F. Xiao, Y. Zhou, J. Zhou, H. Zhu, and X. Niu. Security protocol for rfid system conforming to epc-c1g2 standard. *Journal of Computers*, 8(3), 2013.

[167] F. Xu, Z. Qin, C. Tan, B. Wang, and Q. Li. Imdguard: Securing implantable medical devices with the external wearable guardian. In *INFOCOM, 2011 Proceedings IEEE*, pages 1862 1870, April 2011.

[168] K. Yang, X. Jia, K. Ren, and B. Zhang. Dac-macs: Effective data access control for multi-authority cloud storage systems. In *INFOCOM, 2013 Proceedings IEEE*, pages 2895 2903, April 2013.

[169] M. H. Yang. Secure multiple group ownership transfer protocol for mobile rfid. *Electronic Commerce Research and Applications*, 11(4):361 373, 2012.

[170] W. Yao, C.-H. Chu, and Z. Li. The use of rfid in healthcare: Benefits and barriers. In *RFID-Technology and Applications (RFID-TA), 2010 IEEE International Conference on*, pages 128 134, june 2010.

[171] W. Yao, C.-H. Chu, and Z. Li. Leveraging complex event processing for smart hospitals using rfid. *Journal of Network and Computer Applications*, 34(3):799 810, 2011.

[172] W. Yao, C.-H. Chu, and Z. Li. The adoption and implementation of rfid technologies in healthcare: A literature review. *Journal of Medical Systems*, 36(6):3507 3525, 2012.

[173] T.-C. Yeh, Y.-J. Wang, T.-C. Kuo, and S.-S. Wang. Securing {RFID} systems conforming to {EPC} class 1 generation 2 standard. *Expert Systems with Applications*, 37(12):7678 7683, 2010.

[174] Y.-C. Yen, N.-W. Lo, and T.-C. Wu. Two rfid-based solutions for secure inpatient medication administration. *Journal of Medical Systems*, 36(5):2769 2778, 2012.

[175] X. Yi, J. Willemson, and F. Nait-Abdesselam. Privacy-preserving wireless medical sensor network. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on*, pages 118 125, July 2013.

[176] C. Yoon, D. Kim, W. Jung, C. Kang, and H. Cha. Appscope: Application energy metering framework for android smartphone using kernel activity monitoring. In *USENIX Annual Technical Conference*, 2012.

[177] E.-J. Yoon. Improvement of the securing RFID systems conforming to EPC class 1 generation 2 standard. *Expert Systems with Applications*, 39(1):1589 1594, 2012.

[178] S. Yu, K. Ren, and W. Lou. Fdac: Toward fine-grained distributed data access control in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 22(4):673 686, 2011.

[179] C. Zhang and T.-W. Bae. Vlsi friendly ecg qrs complex detector for body sensor networks. *Emerging and Selected Topics in Circuits and Systems, IEEE Journal on*, 2(1):52 59, March 2012.

[180] Q. Zheng, S. Xu, and G. Ateniese. Vabks: Verifiable attribute-based keyword search over outsourced encrypted data. In *INFOCOM, 2014 Proceedings IEEE*, pages 522 530, April 2014.

[181] W. Zhou, E. J. Yoon, and S. Piramuthu. Simultaneous multi-level rfid tag ownership & transfer in health care environments. *Decision Support Systems*, 54(1):98 108, 2012.

[182] S. Ziauddin and B. Martin. Formal analysis of iso/iec 9798-2 authentication standard using avispa. In *Information Security (Asia JCIS), 2013 Eighth Asia Joint Conference on*, pages 108 114, July 2013.

[183] C. Zulkifli, R. Abdulla, W. Ismail, and M. Rahman. Wireless mesh network in integrated web base monitoring systems for production line automation. In V. Das, E. Ariwa, and S. Rahayu, editors, *Signal Processing and Information Technology*, volume 62 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 7 15. Springer Berlin Heidelberg, 2012.